

Cloud Eye

API Reference

Issue 01
Date 2025-01-20



Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks 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 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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 Before You Start.....	1
1.1 Overview.....	1
1.2 API Calling.....	1
1.3 Endpoints.....	1
1.4 Notes and Constraints.....	1
1.5 Concepts.....	2
2 API Overview.....	3
3 Calling APIs.....	12
3.1 Making an API Request.....	12
3.2 Authentication.....	16
3.3 Response.....	17
4 Getting Started.....	20
5 API V1.....	22
5.1 API Version Management.....	22
5.1.1 Querying All API Versions.....	22
5.1.2 Querying a Specified API Version.....	24
5.2 Metrics.....	27
5.2.1 Querying Metrics.....	27
5.3 Alarm Rules.....	31
5.3.1 Querying Alarm Rules.....	31
5.3.2 Querying Details of an Alarm Rule.....	39
5.3.3 Enabling or Disabling an Alarm Rule.....	45
5.3.4 Deleting an Alarm Rule.....	47
5.3.5 Creating an Alarm Rule.....	48
5.3.6 Creating a Custom Alarm Template.....	58
5.3.7 Deleting a Custom Alarm Template.....	64
5.3.8 Querying the Alarm History of an Alarm Rule.....	65
5.3.9 Querying Custom Alarm Templates.....	76
5.3.10 Updating a Custom Alarm Template.....	83
5.3.11 Modifying an Alarm Rule.....	87
5.4 Monitoring Data.....	95
5.4.1 Querying Monitoring Data of a Metric.....	95

5.4.2 Adding Monitoring Data.....	100
5.4.3 Querying Monitoring Data of Multiple Metrics.....	106
5.4.4 Querying the Host Configuration.....	118
5.5 Quotas.....	121
5.5.1 Querying Quotas.....	121
5.6 Resource Groups.....	123
5.6.1 Querying Resources in a Resource Group.....	123
5.6.2 Creating a Resource Group.....	128
5.6.3 Updating a Resource Group.....	130
5.6.4 Deleting a Resource Group.....	133
5.6.5 Query Resource Groups.....	134
5.7 Event Monitoring.....	139
5.7.1 Reporting Events.....	140
5.7.2 Querying Events.....	145
5.7.3 Querying Details of an Event.....	148
6 API V2.....	155
6.1 Alarm Rules.....	155
6.1.1 Creating an Alarm Rule (Recommended).....	155
6.1.2 Deleting Alarm Rules in Batches.....	166
6.1.3 Enabling or Disabling Alarm Rules in Batches.....	169
6.1.4 Querying Alarm Rules (Recommended).....	172
6.2 Resources in an Alarm Rule.....	182
6.2.1 Batch Adding Resources to an Alarm Rule.....	182
6.2.2 Batch Deleting Resources from an Alarm Rule.....	186
6.2.3 Querying Resources in an Alarm Rule.....	190
6.3 Alarm Policies.....	194
6.3.1 Modifying All Fields in an Alarm Policy.....	194
6.3.2 Querying Alarm Policies.....	203
6.4 Alarm Notifications.....	210
6.4.1 Modifying Alarm Notification Information in an Alarm Rule.....	210
6.5 Alarm Records.....	215
6.5.1 Querying Alarm Records.....	215
6.6 Alarm Templates.....	228
6.6.1 Creating a Custom Alarm Template.....	228
6.6.2 Deleting Custom Alarm Templates in Batches.....	235
6.6.3 Modifying a Custom Alarm Template.....	239
6.6.4 Querying Alarm Templates.....	246
6.6.5 Querying Details of an Alarm Template.....	252
6.7 Alarm Rules Associated with an Alarm Template.....	259
6.7.1 Querying Alarm Rules Associated with an Alarm Template.....	259
6.8 Resource Groups.....	264
6.8.1 This API is used to create a resource group (recommended).....	264

6.8.2 Batch Deleting Resource Groups.....	269
6.8.3 Modifying a Resource Group.....	273
6.8.4 Querying Details of a Resource Group.....	277
6.8.5 Querying Resource Groups.....	283
6.9 Resources in a Resource Group.....	289
6.9.1 Batch Adding Resources to a Resource Group.....	289
6.9.2 Batch Deleting Resources from a Resource Group.....	294
6.9.3 Querying Resources of a Specified Dimension and a Specified Service Type in a Resource Group...	298
6.10 One-Click Monitoring.....	305
6.10.1 Enabling One-Click Monitoring.....	305
6.10.2 Querying Services and Resources That Support One-Click Monitoring.....	311
6.10.3 Querying Alarm Rules of One Service in One-Click Monitoring.....	315
6.10.4 Batch Enabling or Disabling Alarm Rules of One Service in One-Click Monitoring.....	324
6.10.5 Batch Disabling One-Click Motoring.....	328
6.10.6 Batch Modifying Alarm Notifications in Alarm Rules for One Service That Has One-Click Monitoring Enabled.....	332
6.10.7 Batch Enabling or Disabling Alarm Policies in Alarm Rules for One Service That Has One-Click Monitoring Enabled.....	338
6.11 Alarm Notification Masking.....	343
6.11.1 Creating Alarm Notification Masking Rules in Batches.....	343
6.11.2 Modifying the Masking Time of Alarm Notification Masking Rules in Batches.....	348
6.11.3 Modifying an Alarm Notification Masking Rule.....	352
6.11.4 Deleting Alarm Notification Masking Rules in Batches.....	357
6.11.5 Querying Alarm Notification Masking Rules.....	360
6.11.6 Querying Resources for Which Alarm Notifications Have Been Masked.....	372
6.12 Dashboards.....	377
6.12.1 This API is used to create or copy a dashboard.....	377
6.12.2 Querying Dashboards.....	381
6.12.3 Modifying a Dashboard.....	386
6.12.4 This API is used to delete dashboards in batches.....	389
6.13 Graphs.....	393
6.13.1 This API is used to create, copy, or batch create graphs on a dashboard.....	393
6.13.2 Querying Graphs Added to a Dashboard.....	402
6.13.3 Querying Information About a Graph.....	410
6.13.4 Deleting a Graph.....	418
6.13.5 Updating Graphs in Batches.....	421
6.14 Resource Tags.....	430
6.14.1 Querying Tags of a Type of Resources in a Cloud Eye Project.....	430
6.15 Metric Management.....	433
6.15.1 Querying Server Monitoring Metrics from Different Dimensions.....	434
7 API V3.....	439
7.1 Agent Statuses.....	439
7.1.1 Querying Agent Statuses in Batches.....	439

7.2 Agent maintenance tasks.....	445
7.2.1 Querying the Agent Maintenance Tasks.....	445
7.2.2 Creating Agent maintenance Tasks in Batches.....	451
8 Permissions Policies and Supported Actions.....	457
8.1 Introduction.....	457
8.2 Supported Actions of the API Version Management APIs.....	458
8.3 Supported Actions of the Metric Management API.....	459
8.4 Supported Actions of the Alarm Rule Management APIs.....	460
8.5 Supported Actions of the Monitoring Data Management APIs.....	461
8.6 Supported Actions of the Quota Management API.....	462
8.7 Supported Actions of the Event Monitoring API.....	462
9 Common Parameters.....	463
9.1 Status Codes.....	463
9.2 Error Codes.....	464
9.3 Obtaining a Project ID.....	467
A Appendix.....	469
A.1 Services Interconnected with Cloud Eye.....	469
A.2 Events Supported by Event Monitoring.....	473
B Change History.....	572

1 Before You Start

1.1 Overview

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?](#)

1.2 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](#).

1.3 Endpoints

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

1.4 Notes and 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.

1.5 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. 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.
- Enterprise Project
Enterprise projects group and manage resources across regions. Resources in different enterprise projects are logically isolated.
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 versions	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.
	Metrics	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 alarm rules 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 the alarm rule ID.
		Querying Custom Alarm Templates	Query custom alarm templates.
		Updating a Custom Alarm Template	Update a custom alarm template.
		Modifying an Alarm Rule	Modify an alarm rule.
	Monitoring data	Querying Monitoring Data of a Metric	Query the monitoring data of a specified 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 host configuration for a specified event type in a specified time range. You can specify the dimension of data to be queried.
	Quotas	Querying Quotas	Query the alarm rule quota.
	Resource groups	Querying Resources in a Resource Group	Query resources in a resource group based on the 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 the event name.
API V2	Alarm rules	Creating an Alarm Rule (Recommended)	Create an alarm rule.
		Deleting Alarm Rules in Batches	Delete alarm rules in batches.
		Enabling or Disabling Alarm Rules in Batches	Batch enable or disable alarm rules.
		Querying Alarm Rules (Recommended)	Query the alarm rule list.
	Monitored resources	Batch Adding Resources to an Alarm Rule	Batch add resources to an alarm rule. (Alarm rules for resources in resource groups are excluded.)
		Batch Deleting Resources from an Alarm Rule	Batch delete 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	Querying Alarm Records	Query alarm records.
	Alarm templates	Creating a Custom Alarm Template	Create a custom template.
		Deleting Custom Alarm Templates in Batches	Delete custom templates in batches.
		Modifying a Custom Alarm 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	This API is used to create a resource group (recommended).	Create a resource group.
		Batch Deleting Resource Groups	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.
	Resources 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.
	One-click monitoring	Enabling One-Click Monitoring	Enable one-click monitoring.

Type	Subtype	API	Description
		Querying Services and Resources That Support One-Click Monitoring	Query services and resources that support one-click monitoring.
		Querying Alarm Rules of One Service in One-Click Monitoring	Query alarm rules of a service in one-click monitoring.
		Batch Enabling or Disabling Alarm Rules of One Service in One-Click Monitoring	Batch enable or disable alarm rules for a service in one-click monitoring.
		Batch Disabling One-Click Monitoring	Batch disable one-click monitoring.
		Batch Modifying Alarm Notifications in Alarm Rules for One Service That Has 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 Policies in Alarm Rules for One Service That Has 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 notification masking	Creating Alarm Notification Masking Rules in Batches	Create alarm notification masking rules in batches.
		Modifying the Masking Time of Alarm Notification Masking Rules in Batches	Modify the masking time of alarm notification masking rules in batches.
		Modifying an Alarm Notification Masking Rule	Modify an alarm notification masking rule.
		Deleting Alarm Notification Masking Rules in Batches	Delete alarm notification masking rules in batches.
		Querying Alarm Notification Masking Rules	Query notification masking rules of a specified type in batches. Currently, a maximum of 100 notification masking rules can be queried in batches.
		Querying Resources for Which Alarm Notifications Have Been Masked	Query resources for which alarm notifications have been masked.
	Dashboards	This API is used to create or copy a dashboard.	Create or copy a dashboard.
		Querying Dashboards	Query dashboards.
		Modifying a Dashboard	Modify a dashboard.

Type	Subtype	API	Description
		This API is used to delete dashboards in batches.	Delete dashboards in batches.
	Graphs	This API is used to create, copy, or batch create 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 tags	Querying Tags of a Type of Resources in a Cloud Eye Project	Query tags of a type of resources in a Cloud Eye project.
	Metrics	Querying Server Monitoring Metrics from Different Dimensions	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 tasks	Querying the Agent Maintenance Tasks	Query the Agent tasks.

Type	Subtype	API	Description
		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. The obtained token can then be used to authenticate the calling of other APIs.

Request URI

A request URI is in the following format:

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

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

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 Dublin is iam.myhuaweicloud.eu .
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 .

Parameter	Description
query-string	Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of <i>Parameter name=Parameter value</i> . 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 **EU-Dublin** region, obtain the endpoint of IAM (**iam.myhuaweicloud.eu**) 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.myhuaweicloud.eu/v3.0/OS-USER/users`

 **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.myhuaweicloud.eu/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 <i>Hostname:Port number</i> . 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	<p>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).</p> <p>After the request is processed, the value of X-Subject-Token in the response header is the token value.</p>	<p>No</p> <p>This field is mandatory for token authentication.</p>	<p>The following is part of an example token:</p> <p>MIIPAgYJKoZlhvc NAQcCo...ggg1B BIINPXsidG9rZ</p>

 **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.myhuaweicloud.eu/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.myhuaweicloud.eu/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. In the response to the API used to obtain a user token, **X-Subject-Token** is the desired user token. This token can then be used to authenticate the calling of other APIs.

3.2 Authentication

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

- Token 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": "xxxxxxx" //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:

```
POST https://iam.myhuaweicloud.eu/v3/auth/projects  
Content-Type: application/json  
X-Auth-Token: ABCDEFJ....
```

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

In AK/SK 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 3-1 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 3-1 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_██████████_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 is 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-bfdb93d4051"
      }
    ],
    "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	Specifies the 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	Specifies the list of all versions. For details, see Table 5-6 .

Table 5-6 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 5-7 .
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 5-7 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

```
{
  "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.

URI

GET /V1.0/{project_id}/metrics

- Parameter description

Table 5-8 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 .

Table 5-9 Query parameter description

Parameter	Mandatory	Type	Description
namespace	No	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 (_).

Parameter	Mandatory	Type	Description
metric_name	No	String	Specifies the metric ID. For example, if the monitoring metric of an ECS is CPU usage, metric_name is cpu_util . For details, see Services Interconnected with Cloud Eye .
dim	No	String	Specifies the dimension. For example, the ECS dimension is instance_id . For details about each service dimension, see Services Interconnected with Cloud Eye . A maximum of three dimensions are supported, and the dimensions are numbered from 0 in dim.{i}=key,value format. key cannot exceed 32 characters and value cannot exceed 256 characters. Single dimension: dim.0=instance_id,6f3c6f91-4b24-4e1b-b7d1-a94ac1cb011d Multiple dimensions: dim.0=key,value&dim.1=key,value
start	No	String	Specifies the paging start value. The format is namespace.metric_name.key: value . Example: start=SYS.ECS.cpu_util.instance_id:d9112af5-6913-4f3b-bd0a-3f96711e004d .
limit	No	Integer	Supported range: 1 to 1000 (default) This parameter is used to limit the number of query results.

Parameter	Mandatory	Type	Description
order	No	String	Specifies the result sorting method, which is sorted by timestamp. The default method is desc . <ul style="list-style-type: none"> asc: The query results are displayed in the ascending order. desc: The query results are displayed in the descending order.

- 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	Specifies the list of metric objects. For details, see Table 5-11 .
meta_data	Object	Specifies the 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	Specifies the metric namespace.

Parameter	Type	Description
dimensions	Array of objects	Specifies the list of metric dimensions. For details, see Table 5-12 .
metric_name	String	Specifies the metric name, such as cpu_util .
unit	String	Specifies the metric unit.

Table 5-12 dimensions data structure description

Parameter	Type	Description
name	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 .
value	String	Specifies the dimension value, for example, an ECS ID. Enter 1 to 256 characters.

Table 5-13 meta_data data structure description

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

- 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.

URI

GET /V1.0/{project_id}/alarms

- Parameter description

Table 5-14 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 .

Table 5-15 Parameter description

Parameter	Type	Description
alarms	Array of objects	Specifies the alarm rule list. For details, see Table 5-16 .

Table 5-16 Query parameter description

Parameter	Mandatory	Type	Description
start	No	String	Specifies the first queried alarm to be displayed on a page. The value is alarm_id .
limit	No	Integer	Supported range: 1 to 100 (default) This parameter is used to limit the number of query results.
order	No	String	Specifies the result sorting method, which is sorted by timestamp. The default method is desc . <ul style="list-style-type: none"> • asc: The query results are displayed in the ascending order. • desc: The query results are displayed in the descending order.

- 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 5-17 Parameter description

Parameter	Type	Description
metric_alarms	Array of objects	Specifies the list of alarm objects. For details, see Table 5-18 .
meta_data	Object	Specifies the metadata of query results, including the pagination information. For details, see Table 5-24 .

Table 5-18 metric_alarms data structure description

Parameter	Type	Description
alarm_name	String	Specifies the alarm rule name.
alarm_description	String	Provides supplementary information about the alarm rule.
metric	Object	Specifies the alarm metric. For details, see Table 5-19 .
condition	Object	Specifies the alarm triggering condition. For details, see Table 5-23 .
alarm_enabled	Boolean	Specifies whether to enable the alarm rule.
alarm_level	Integer	Specifies the alarm severity, which can be 1 , 2 (default), 3 or 4 , indicating critical, major, minor, and informational, respectively.
alarm_action_enabled	Boolean	Specifies whether to enable the action to be triggered by an alarm.
alarm_actions	Array of objects	Specifies the action to be triggered by an alarm. For details, see Table 5-21 .

Parameter	Type	Description
ok_actions	Array of objects	Specifies the action to be triggered after the alarm is cleared. For details, see Table 5-22 .
alarm_id	String	Specifies the alarm rule ID.
update_time	Long	Specifies when the alarm status changed. The time is a UNIX timestamp and the unit is ms.
alarm_state	String	Specifies the alarm status, which can be <ul style="list-style-type: none"> • ok: The alarm status is normal. • alarm: An alarm is generated. • insufficient_data: The required data is insufficient.

Table 5-19 metric data structure description

Parameter	Type	Description
namespace	String	Specifies the namespace of a service. For details, see Services Interconnected with Cloud Eye .
dimensions	Array of objects	Specifies the list of metric dimensions. For details, see Table 5-20 .
metric_name	String	Specifies the metric ID. For example, if the monitoring metric of an ECS is CPU usage, metric_name is cpu_util . For details, see Services Interconnected with Cloud Eye .
resource_group_id	String	Specifies the resource group ID selected during the alarm rule creation, for example, rg1603786526428bWbVmk4rP .
resource_group_name	String	Specifies the name of the resource group selected during the alarm rule creation, for example, Resource-Group-ECS-01 .

Table 5-20 dimensions data structure description

Parameter	Type	Description
name	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 .

Parameter	Type	Description
value	String	Specifies the dimension value, for example, an ECS ID. Enter 1 to 256 characters.

Table 5-21 alarm_actions data structure description

Parameter	Type	Description
type	String	Specifies the alarm notification type. <ul style="list-style-type: none"> • notification: indicates that a notification will be sent. • autoscaling: indicates that a scaling action will be triggered.
notificationList	Array of strings	Specifies the list of objects to be notified if the alarm status changes. NOTE The IDs in the list are strings.

Table 5-22 ok_actions data structure description

Parameter	Type	Description
type	String	Specifies the notification type when an alarm is triggered. <ul style="list-style-type: none"> • notification: indicates that a notification will be sent. • autoscaling: indicates that a scaling action will be triggered.
notificationList	Array of strings	Specifies the ID list of objects to be notified if the alarm status changes. NOTE The IDs in the list are strings.

Table 5-23 condition data structure description

Parameter	Type	Description
period	Integer	Specifies the interval (seconds) for checking whether the configured alarm rules are met.

Parameter	Type	Description
filter	String	Specifies the data rollup method, which can be <ul style="list-style-type: none"> • average: Cloud Eye calculates the average value of metric data within a rollup period. • max: Cloud Eye calculates the maximum value of metric data within a rollup period. • min: Cloud Eye calculates the minimum value of metric data within a rollup period. • sum: Cloud Eye calculates the sum of metric data within a rollup period. • variance: Cloud Eye calculates the variance value of metric data within a rollup period.
comparison_operator	String	Specifies the alarm threshold operator, which can be >, =, <, >=, or <=.
value	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 <code>cpu_util</code> in Services Interconnected with Cloud Eye to 80 .
unit	String	Specifies the data unit. Enter up to 32 characters.
count	Integer	Specifies the number of consecutive occurrence times that the alarm policy was met. Supported range: 1 to 5

Parameter	Type	Description
suppress_duration	Integer	<p>Specifies the interval for triggering an alarm if the alarm persists.</p> <p>Possible intervals are as follows:</p> <p>0: Cloud Eye triggers the alarm only once.</p> <p>300: Cloud Eye triggers the alarm every 5 minutes.</p> <p>600: Cloud Eye triggers the alarm every 10 minutes.</p> <p>900: Cloud Eye triggers the alarm every 15 minutes.</p> <p>1800: Cloud Eye triggers the alarm every 30 minutes.</p> <p>3600: Cloud Eye triggers the alarm every hour.</p> <p>10800: Cloud Eye triggers the alarm every 3 hours.</p> <p>21600: Cloud Eye triggers the alarm every 6 hours.</p> <p>43200: Cloud Eye triggers the alarm every 12 hours.</p> <p>86400: Cloud Eye triggers the alarm every day.</p>

Table 5-24 meta_data data structure description

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

- Example response

```

{
  "metric_alarms": [
    {
      "alarm_name": "alarm-tttttt",
      "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-m5rwx",
    "alarm_description": "",
    "metric": {
        "namespace": "SYS.ECS",
        "dimensions": [
            {
                "name": "instance_id",
                "value": "30f3858d-4377-4514-9081-be5bdf1392e"
            }
        ],
        "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.
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.

URI

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

- Parameter description

Table 5-25 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 .

Parameter	Mandatory	Description
alarm_id	Yes	Specifies the 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	Specifies the list of alarm objects. For details, see Table 5-26 .

Table 5-26 metric_alarms data structure description

Parameter	Type	Description
alarm_name	String	Specifies the alarm rule name.
alarm_description	String	Provides supplementary information about the alarm rule.
metric	Object	Specifies the alarm metric. For details, see Table 5-27 .
condition	Object	Specifies the alarm triggering condition. For details, see Table 5-31 .
alarm_enabled	Boolean	Specifies whether to enable the alarm rule.
alarm_level	Integer	Specifies the alarm severity, which can be 1 , 2 (default), 3 or 4 , indicating critical, major, minor, and informational, respectively.
alarm_action_enabled	Boolean	Specifies whether to enable the action to be triggered by an alarm.
alarm_actions	Array of objects	Specifies the action to be triggered by an alarm. For details, see Table 5-29 .
ok_actions	Array of objects	Specifies the action to be triggered after the alarm is cleared. For details, see Table 5-30 .

Parameter	Type	Description
alarm_id	String	Specifies the alarm rule ID.
update_time	Long	Specifies when the alarm status changed. The time is a UNIX timestamp and the unit is ms.
alarm_state	String	Specifies the alarm status, which can be <ul style="list-style-type: none"> • ok: The alarm status is normal. • alarm: An alarm is generated. • insufficient_data: The required data is insufficient.

Table 5-27 metric data structure description

Parameter	Type	Description
namespace	String	Specifies the namespace of a service. For details, see Services Interconnected with Cloud Eye .
dimensions	Array of objects	Specifies the list of metric dimensions. For details, see Table 5-28 .
metric_name	String	Specifies the metric ID. For example, if the monitoring metric of an ECS is CPU usage, metric_name is cpu_util . For details, see Services Interconnected with Cloud Eye .
resource_group_id	String	Specifies the resource group ID selected during the alarm rule creation, for example, rg1603786526428bWbVmk4rP .
resource_group_name	String	Specifies the 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	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 .
value	String	Specifies the 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	Specifies the alarm notification type. <ul style="list-style-type: none"> • notification: indicates that a notification will be sent. • autoscaling: indicates that a scaling action will be triggered.
notificationList	Array of strings	Specifies the list of objects to be notified if the alarm status changes. NOTE The IDs in the list are strings.

Table 5-30 ok_actions data structure description

Parameter	Type	Description
type	String	Specifies the notification type when an alarm is triggered. <ul style="list-style-type: none"> • notification: indicates that a notification will be sent. • autoscaling: indicates that a scaling action will be triggered.
notificationList	Array of strings	Specifies the list of objects to be notified if the alarm status changes. NOTE The IDs in the list are strings.

Table 5-31 condition data structure description

Parameter	Type	Description
period	Integer	Specifies the interval (seconds) for checking whether the configured alarm rules are met.

Parameter	Type	Description
filter	String	Specifies the data rollup method, which can be <ul style="list-style-type: none">• average: Cloud Eye calculates the average value of metric data within a rollup period.• max: Cloud Eye calculates the maximum value of metric data within a rollup period.• min: Cloud Eye calculates the minimum value of metric data within a rollup period.• sum: Cloud Eye calculates the sum of metric data within a rollup period.• variance: Cloud Eye calculates the variance value of metric data within a rollup period.
comparison_operator	String	Specifies the alarm threshold operator, which can be >, =, <, >=, or <=.
value	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 <code>cpu_util</code> in Services Interconnected with Cloud Eye to 80 .
unit	String	Specifies the data unit. Enter up to 32 characters.
count	Integer	Specifies the number of consecutive occurrence times that the alarm policy was met. Supported range: 1 to 5

Parameter	Type	Description
suppress_duration	Integer	<p>Specifies the interval for triggering an alarm if the alarm persists.</p> <p>Possible intervals are as follows:</p> <p>0: Cloud Eye triggers the alarm only once.</p> <p>300: Cloud Eye triggers the alarm every 5 minutes.</p> <p>600: Cloud Eye triggers the alarm every 10 minutes.</p> <p>900: Cloud Eye triggers the alarm every 15 minutes.</p> <p>1800: Cloud Eye triggers the alarm every 30 minutes.</p> <p>3600: Cloud Eye triggers the alarm every hour.</p> <p>10800: Cloud Eye triggers the alarm every 3 hours.</p> <p>21600: Cloud Eye triggers the alarm every 6 hours.</p> <p>43200: Cloud Eye triggers the alarm every 12 hours.</p> <p>86400: Cloud Eye triggers the alarm every day.</p>

- 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": "a11498096535573r8DNy7Gyk",
  "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.

URI

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

- Parameter description

Table 5-32 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/al1441967036681YkazZ0deN/action
```

Request

- Request parameters

Table 5-33 Request parameters

Parameter	Mandatory	Type	Description
alarm_enabled	Yes	Boolean	Specifies whether the alarm rule is enabled. <ul style="list-style-type: none">• true: indicates that the alarm rule is enabled.• false: indicates that the alarm rule is disabled.

- 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.

URI

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

- Parameter description

Table 5-34 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.

URI

POST /V1.0/{project_id}/alarms

- 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 .

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

Request

- Request parameters

Table 5-36 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 5-37 .
condition	Yes	Object	Specifies the alarm triggering condition. For details, see Table 5-42 .
alarm_enabled	No	Boolean	Specifies whether to enable the alarm. The default value is true .
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 .)

Parameter	Mandatory	Type	Description
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: <pre>{ "type": "notification","notificationList" : ["urn:smn:region:68438a86d9 8e427e907e0097b7e35d47:sd"] }</pre> For details, see Table 5-39 .
ok_actions	No	Array of objects	Specifies the action to be triggered after the alarm is cleared. Its structure is: <pre>{ "type": "notification","notificationList" : ["urn:smn:region:68438a86d9 8e427e907e0097b7e35d47:sd"] }</pre> For details, see Table 5-40 .

Parameter	Mandatory	Type	Description
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: <pre>{ "type": "notification", "notificationList": ["urn:smn:region:68438a86d98e427e907e0097b7e35d47:sd"] }</pre> For details, see Table 5-41 .

Table 5-37 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 5-38 .
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 5-38 dimensions data structure description

Parameter	Mandatory	Type	Description
name	Yes	String	<p>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.</p> <p>Start with a letter. Enter 1 to 32 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.</p>
value	Yes	String	<p>Specifies the dimension value, for example, an ECS ID.</p> <p>Specifies the dimension value, for example, an ECS ID.</p> <p>Start with a letter or a digit. Enter 1 to 256 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.</p>

Table 5-39 alarm_actions data structure description

Parameter	Mandatory	Type	Description
type	Yes	String	<p>Specifies the alarm notification type.</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>If you set type to notification, you must specify notificationList. If you set type to autoscaling, you must set notificationList to [].</p> <p>NOTE</p> <ul style="list-style-type: none"> To make the Auto Scaling (AS) alarm rule take effect, 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 5-40 ok_actions data structure description

Parameter	Mandatory	Type	Description
type	Yes	String	<p>Specifies the notification type when an alarm is triggered.</p> <ul style="list-style-type: none"> 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	<p>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.</p> <p>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.)</p> <p>If alarm_actions and ok_actions coexist, their notificationList must be the same. (You do not need to configure the deprecated parameter insufficientdata_actions.)</p>

Table 5-41 insufficientdata_actions data structure description

Parameter	Mandatory	Type	Description
type	Yes	String	<p>Specifies the notification type when an alarm is triggered.</p> <ul style="list-style-type: none"> • notification: indicates that a notification will be sent. • autoscaling: indicates that a scaling action will be triggered.
notificationList	Yes	Array of objects	<p>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.</p> <p>NOTE</p> <ul style="list-style-type: none"> • 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 5-42 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 <ul style="list-style-type: none"> 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	<p>Specifies the interval for triggering an alarm if the alarm persists.</p> <p>Possible intervals are as follows:</p> <p>0: Cloud Eye triggers the alarm only once.</p> <p>300: Cloud Eye triggers the alarm every 5 minutes.</p> <p>600: Cloud Eye triggers the alarm every 10 minutes.</p> <p>900: Cloud Eye triggers the alarm every 15 minutes.</p> <p>1800: Cloud Eye triggers the alarm every 30 minutes.</p> <p>3600: Cloud Eye triggers the alarm every hour.</p> <p>10800: Cloud Eye triggers the alarm every 3 hours.</p> <p>21600: Cloud Eye triggers the alarm every 6 hours.</p> <p>43200: Cloud Eye triggers the alarm every 12 hours.</p> <p>86400: Cloud Eye triggers the alarm every day.</p>

- 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-bfdb93d4051"
      }
    ],
    "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 5-43 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.

URI

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

- Parameter description

Table 5-44 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 5-45 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 5-46 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 5-47 .
alarm_level	No	Integer	Specifies the alarm severity. Possible severities are 1 (critical), 2 (major), 3 (minor), and 4 (informational).

Table 5-47 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	<p>Specifies the period during which Cloud Eye determines whether to trigger an alarm.</p> <p>Unit: second</p> <p>Possible periods are 1, 300, 1200, 3600, 14400, and 86400.</p> <p>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).</p>
unit	No	String	<p>Specifies the data unit. Enter up to 32 characters.</p>
value	Yes	Double	<p>Specifies the alarm threshold, which ranges from 0 to Number.</p> <p>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.</p>

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

- 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 5-48 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.

URI

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

- Parameter description

Table 5-49 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.
403 Forbidden	Access to the requested page is forbidden.
408 Request Timeout	The request timed out.
429 Too Many Requests	Concurrent requests are excessive.

Returned Value	Description
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.

URI

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

- 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 .
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 .
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 .

Parameter	Mandatory	Description
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 5-51 .
meta_data	MetaData object	No	Specifies the total number of query results returned. For details, see Table 5-60 .

Table 5-51 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 5-52 .
condition	Condition object	No	Specifies the alarm policy set in the alarm rule. For details, see Table 5-57 .
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
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 .

Parameter	Type	Mandatory	Description
alarm_actions	Array of objects	No	<p>Specifies the action to be triggered by an alarm. The structure is as follows:</p> <pre>{ "type": "notification", "notificationList": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"] }</pre> <p>The value of type can be one of the following:</p> <p>notification: indicates that a notification will be sent.</p> <p>autoscaling: indicates that a scaling action will be triggered.</p> <p>notificationList: indicates the list of objects to be notified if the alarm status changes.</p> <p>For details, see Table 5-54.</p>
ok_actions	Array of objects	No	<p>Specifies the action to be triggered after the alarm is cleared. The structure is as follows: {"type": "notification", "notificationList": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"] }</p> <p>The value of type can be one of the following:</p> <p>notification: indicates that a notification will be sent.</p> <p>notificationList: indicates the list of objects to be notified if the alarm status changes.</p> <p>For details, see Table 5-55.</p>
insufficientdata_actions	Array of objects	No	<p>Specifies the action triggered by data insufficiency. The structure is as follows: {"type": "notification", "notificationList": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"]}</p> <p>The value of type can be one of the following:</p> <p>notification: An alarm is triggered due to insufficient data.</p> <p>notificationList: Specifies the ID list of the notification objects when an alarm notification is triggered due to insufficient data.</p> <p>For details, see Table 5-56.</p>

Parameter	Type	Mandatory	Description
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 5-58 .
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 5-59 .

Table 5-52 metric data structure description

Parameter	Type	Mandatory	Description
dimensions	Array of objects	No	Specifies the metric dimension. For details, see Table 5-53 .
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 .

Parameter	Type	Mandatory	Description
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 5-53 dimensions data structure description

Parameter	Type	Mandatory	Description
name	String	No	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 .
value	String	No	Specifies the dimension value, for example, an ECS ID. Enter 1 to 256 characters.

Table 5-54 alarm_actions data structure description

Parameter	Type	Mandatory	Description
type	String	Yes	Specifies the alarm notification type. <ul style="list-style-type: none"> 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 5-55 ok_actions data structure description

Parameter	Type	Mandatory	Description
type	String	Yes	Specifies the alarm notification type. <ul style="list-style-type: none"> • 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 insufficientdata_actions data structure description

Parameter	Type	Mandatory	Description
type	String	Yes	Specifies the alarm notification type. <ul style="list-style-type: none"> • 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 condition data structure description

Parameter	Type	Man dato ry	Description
period	Integer	No	<p>Specifies how often Cloud Eye aggregates data, which can be</p> <ul style="list-style-type: none"> • 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. <p>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).</p>
filter	String	No	<p>Specifies the data rollup method, which can be</p> <ul style="list-style-type: none"> • average: Cloud Eye calculates the average value of metric data within a rollup period. • max: Cloud Eye calculates the maximum value of metric data within a rollup period. • min: Cloud Eye calculates the minimum value of metric data within a rollup period. • sum: Cloud Eye calculates the sum of metric data within a rollup period. • variance: Cloud Eye calculates the variance value of metric data within a rollup period.
comparison_ operator	String	No	<p>Specifies the alarm threshold operator, which can be >, =, <, >=, or <=.</p>

Parameter	Type	Mandatory	Description
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 5-58 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 5-59 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 5-60 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": "al1604473978613MvvlbVZD",
  "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": "rg160447397837330303XQbK",
  "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.

URI

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

- Parameter description

Table 5-61 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 5-62 .
meta_data	MetaData object	No	Specifies the metadata of query results, including the pagination information. For details, see Table 5-65 .

Table 5-62 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 5-63 .
template_id	String	No	Specifies the ID of the custom alarm template, for example, at1603330892378wkDm77y6B .

Table 5-63 template_items data structure description

Parameter	Type	Man dato ry	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 5-64 .
alarm_level	Integer	No	Specifies the alarm severity, which can be 1 (critical), 2 (major), 3 (minor), or 4 (informational).

Table 5-64 condition data structure description

Parameter	Type	Man dato ry	Description
period	Integer	Yes	Specifies how often Cloud Eye aggregates data. Possible values: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • average: Cloud Eye calculates the average value of metric data within a rollup period. • max: Cloud Eye calculates the maximum value of metric data within a rollup period. • min: Cloud Eye calculates the minimum value of metric data within a rollup period. • sum: Cloud Eye calculates the sum of metric data within a rollup period. • variance: Cloud Eye calculates the variance value of metric data within a rollup 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 5-65 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.

URI

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

- Parameter description

Table 5-66 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 5-67 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.

Parameter	Mandatory	Type	Description
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 5-68 .

Table 5-68 `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 5-69 .
alarm_level	No	Integer	Specifies the alarm severity. Possible severities are 1 (critical), 2 (major), 3 (minor), and 4 (informational).

Table 5-69 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: <ul style="list-style-type: none"> • 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 <code>cpu_util</code> to 80 .

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

- 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.

URI

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

- Parameter description

Table 5-70 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 5-71 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 5-72 .
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.

Parameter	Mandatory	Type	Description
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 5-73 .
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 5-75 .
ok_actions	No	Array of objects	Specifies the action to be triggered after the alarm is cleared. For details, see Table 5-74 .

Table 5-72 condition data structure description

Parameter	Mandatory	Type	Description
period	Yes	Integer	Specifies how often Cloud Eye aggregates data, which can be <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • average: Cloud Eye calculates the average value of metric data within a rollup period. • max: Cloud Eye calculates the maximum value of metric data within a rollup period. • min: Cloud Eye calculates the minimum value of metric data within a rollup period. • sum: Cloud Eye calculates the sum of metric data within a rollup period. • variance: Cloud Eye calculates the variance value of metric data within a rollup 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 .

Parameter	Mandatory	Type	Description
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
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 5-73 alarm_actions data structure description

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the alarm notification type. <ul style="list-style-type: none"> • 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	<p>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.</p> <p>If you set type to notification, you must specify notificationList. If you set type to autoscaling, you must set notificationList to [].</p> <p>NOTE</p> <ul style="list-style-type: none"> To make the Auto Scaling (AS) alarm rule take effect, 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 5-74 ok_actions data structure description

Parameter	Mandatory	Type	Description
type	Yes	String	<p>Specifies the notification type when an alarm is triggered.</p> <ul style="list-style-type: none"> 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	<p>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.</p> <p>NOTE</p> <p>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.)</p> <p>If alarm_actions and ok_actions coexist, their notificationList must be the same. (You do not need to configure the deprecated parameter insufficientdata_actions.)</p>

Table 5-75 insufficientdata_actions data structure description

Parameter	Mandatory	Type	Description
type	Yes	String	<p>Specifies the notification type when an alarm is triggered.</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>NOTE</p> <ul style="list-style-type: none"> 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.

URI

```
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 5-76 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 .

Table 5-77 Query parameter 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 (_).
metric_name	Yes	String	Specifies the metric name. You can obtain the metric names of existing alarm rules by referring to Querying Metrics .
from	Yes	String	Specifies the start time of the query. The time is a UNIX timestamp and the unit is ms. Rollup aggregates the raw data generated within a period to the start time of the period. If from and to are within a period, the query result will be empty due to the rollup failure. 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. NOTE Cloud Eye rounds up from based on the level of granularity required to perform the rollup.
to	Yes	String	Specifies the end time of the query. The time is a UNIX timestamp and the unit is ms. from must be earlier than to .

Parameter	Mandatory	Type	Description
period	Yes	Integer	<p>Specifies how often Cloud Eye aggregates data, which can be</p> <ul style="list-style-type: none"> • 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	<p>Specifies the data rollup method, which can be</p> <ul style="list-style-type: none"> • average: Cloud Eye calculates the average value of metric data within a rollup period. • max: Cloud Eye calculates the maximum value of metric data within a rollup period. • min: Cloud Eye calculates the minimum value of metric data within a rollup period. • sum: Cloud Eye calculates the sum of metric data within a rollup period. • variance: Cloud Eye calculates the variance value of metric data within a rollup period. <p>NOTE Rollup uses a rollup method to aggregate raw data generated within a specific period. 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.</p>

Parameter	Mandatory	Type	Description
dim	Yes	String	<p>A maximum of three metric dimensions are supported, and the dimensions are numbered from zero in the dim.{i}=key,value format. key cannot exceed 32 characters and value cannot exceed 256 characters.</p> <p>The following dimensions are only examples. For details about whether multiple dimensions are supported, see the dimension description in the monitoring indicator description of each service.</p> <p>Single dimension: dim.0=instance_id,i-12345</p> <p>Multiple dimensions: dim.0=instance_id,i-12345&dim.1=instance_name,i-1234</p>

 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 5-78 Parameter description

Parameter	Type	Description
datapoints	Array of objects	Specifies the metric data list. For details, see Table 5-79 . 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	Specifies the metric ID. For example, if the monitoring metric of an ECS is CPU usage, metric_name is cpu_util . For details, see Services Interconnected with Cloud Eye .

Table 5-79 datapoints data structure description

Parameter	Type	Description
average	Double	Specifies the average value of metric data within a rollup period.
max	Double	Specifies the maximum value of metric data within a rollup period.
min	Double	Specifies the minimum value of metric data within a rollup period.
sum	Double	Specifies the sum of metric data within a rollup period.
variance	Double	Specifies the variance of metric data within a rollup period.
timestamp	Long	Specifies when the metric is collected. It is a UNIX timestamp in milliseconds.
unit	String	Specifies the metric unit.

- 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*.

URI

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

- Parameter description

Table 5-80 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}/metric-data

For details about Cloud Eye endpoints, go to [Endpoints](#) to query the URL of each region.

Request

NOTICE

- The size of a POST request cannot exceed 512 KB. Otherwise, the request will be denied.
- 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.
- 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 5-81 Parameter description

Parameter	Type	Mandatory	Description
Array elements	Array of objects	Yes	Specifies whether to add one or more pieces of custom metric monitoring data. For details, see Table 5-82 .

Table 5-82 Array elements

Parameter	Mandatory	Type	Description
metric	Yes	Object	Specifies the metric data. For details, see Table 5-83 .
ttl	Yes	Integer	Specifies the data validity period. The unit is second. Supported range: 1 to 604800 If the validity period expires, the data will be automatically deleted.
collect_time	Yes	Long	Specifies when the data was collected. The time is UNIX timestamp (ms) format. NOTE Since there is a latency between the client and the server, the data timestamp to be inserted should be within the period that starts from three days before the current time plus 20s to 10 minutes after the current time minus 20s. In this way, the timestamp will be inserted to the database without being affected by the latency.
value	Yes	Double	Specifies the monitoring metric data to be added, which can be an integer or a floating point number.
unit	No	String	Specifies the data unit. Enter a maximum of 32 characters.
type	No	String	Specifies the enumerated type. Possible types: <ul style="list-style-type: none">• int• float

Table 5-83 metric data structure description

Parameter	Mandatory	Type	Description
namespace	Yes	String	<p>Specifies the customized namespace. For details, see Services Interconnected with Cloud Eye.</p> <p>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 (_). In addition, service cannot start with SYS, AGT, or SRE, and namespace cannot be SERVICE.BMS because this namespace has been used by the system.</p> <p>You can leave this parameter blank when you set alarm_type to (EVENT.SYS EVENT.CUSTOM).</p>
dimensions	Yes	Array of objects	<p>Specifies the metric dimension. A maximum of three dimensions are supported.</p> <p>For details, see Table 5-84.</p>
metric_name	Yes	String	<p>Specifies the metric ID. For example, if the monitoring metric of an ECS is CPU usage, metric_name is cpu_util. For details, see Services Interconnected with Cloud Eye.</p>

Table 5-84 dimensions data structure description

Parameter	Mandatory	Type	Description
name	Yes	String	<p>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.</p> <p>Start with a letter. Enter 1 to 32 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.</p>

Parameter	Mandatory	Type	Description
value	Yes	String	Specifies the dimension value, for example, an ECS ID. Start with a letter or a digit. Enter 1 to 256 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.

- 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 **dc_instance_id** is **1598b5d4-3cb5-4f4d-8d99-2425d8e9ed54** and **dc_cluster_redis_node** is **6666cd76f96956469e7be39d750cc7d9**.

```

[
  {
    "metric": {
      "namespace": "SYS.DCS",
      "dimensions": [
        {
          "name": "dc_instance_id",
          "value": "1598b5d4-3cb5-4f4d-8d99-2425d8e9ed54"
        },
        {
          "name": "dc_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.

Returned Value	Description
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 monitoring 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.

URI

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

- Parameter description

Table 5-85 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 .

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 5-86 Request parameters

Parameter	Mandatory	Type	Description
metrics	Yes	Array of objects	Specifies the metric data. The maximum length of the array is 500. For details, see Table 5-87 .

Parameter	Mandatory	Type	Description
from	Yes	Long	<p>Specifies the start time of the query. The time is a UNIX timestamp and the unit is ms. Set from to at least one period earlier than the current time. Rollup aggregates the raw data generated within a period to the start time of the period. If from and to are within a period, the query result will be empty due to the rollup failure. 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.</p> <p>NOTE Cloud Eye rounds up from based on the level of granularity required to perform the rollup.</p>
to	Yes	Long	<p>Specifies the end time of the query. The time is a UNIX timestamp and the unit is ms. from must be earlier than to.</p>
period	Yes	String	<p>Specifies how often Cloud Eye aggregates data, which can be</p> <ul style="list-style-type: none"> • 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.

Parameter	Mandatory	Type	Description
filter	Yes	String	<p>Specifies the data rollup method, which can be</p> <ul style="list-style-type: none"> • average: Cloud Eye calculates the average value of metric data within a rollup period. • max: Cloud Eye calculates the maximum value of metric data within a rollup period. • min: Cloud Eye calculates the minimum value of metric data within a rollup period. • sum: Cloud Eye calculates the sum of metric data within a rollup period. • variance: Cloud Eye calculates the variance value of metric data within a rollup period. <p>filter does not affect the query result of raw data. (The period is 1.)</p>

Table 5-87 metrics data structure description

Parameter	Mandatory	Type	Description
namespace	Yes	String	<p>Specifies the namespace of a service. For details, see Services Interconnected with Cloud Eye.</p> <p>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 (_).</p>
metric_name	Yes	String	<p>Specifies the metric ID. For example, if the monitoring metric of an ECS is CPU usage, metric_name is cpu_util. For details, see Services Interconnected with Cloud Eye.</p> <p>The value must start with a letter. Enter 1 to 64 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.</p>

Parameter	Mandatory	Type	Description
dimensions	Yes	Array of objects	Specifies metric dimensions. dimensions is an array consisting of a maximum of four JSON objects. One dimension is a JSON object, and its structure is as follows: <pre>{ "name": "instance_id", "value": "33328f02-3814-422e-b688-bfdb93d4050" }</pre> For details, see Table 5-88 .

Table 5-88 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 . Start with a letter. Enter 1 to 32 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.
value	Yes	String	Specifies the dimension value, for example, an ECS ID. dimensions can be obtained from the response body by calling the API for querying metrics . Start with a letter or a digit. Enter 1 to 256 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.

 **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

Request example 1: Query the average disk usage of the OS on the ECS whose **instance_id** is **07d878a9-2243-4e84-aeef-c47747d18024** and **mount_point** is **012bec14bc176310c19f40e384fd629b** 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"
  }]
}
```

Request example 2: Query the average memory usage of the OS 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"
  }]
}
```

Request example 3: Query the average **cpu_util** of the five ECSs whose **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 36,000,000. The value of the request parameter (**to-from**) is 86,399,000, which exceeds the maximum value 36,000,000. The formula is as follows: The number of metrics × (**to-from**)/Monitoring period ≤ 3000. The value of **from** in the request parameter is automatically changed to **to-36,000,000**, that is, 1,724,219,999,000.

```
{
  "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"
}
```

Request 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**. The monitoring data was collected 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"
}

```

Request example 5: View the 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**. The monitoring data was collected 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 request 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 rollup period is 20 minutes.

```

{
  "metrics": [
    {
      "namespace": "AGT.ECS",
      "dimensions": [
        {
          "name": "instance_id",
          "value": "cd841102-f6b1-407d-a31f-235db796dcbb"
        },
        {
          "name": "proc",
          "value": "b28354b543375bfa94dabaeda722927f"
        }
      ],
      "metric_name": "proc_specified_count"
    }
  ],
}

```



```

"from": 1556625600000,
"to": 1556632800000,
"period": "1200",
"filter": "min"
}

```

Response

- Response parameters

Table 5-89 Parameter description

Parameter	Type	Description
metrics	Array of objects	Specifies the metric data. For details, see Table 5-90 .

Table 5-90 metrics data structure description

Parameter	Type	Description
unit	String	Specifies the metric unit.
datapoints	Array of objects	Specifies the metric data list. Cloud Eye rounds up the value of from based on the selected granularity for data query, so datapoints may contain more data points than expected. Up to 3,000 data points can be returned. For details, see Table 5-92 .
namespace	String	Specifies the metric namespace, which 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	Array of objects	Specifies the list of metric dimensions. Each dimension is a JSON object, and its structure is as follows: <pre> { "name": "instance_id", "value": "33328f02-3814-422e-b688-bfdb93d4050" } </pre> For details, see Table 5-91 .
metric_name	String	Specifies the metric name. Start with a letter. Enter 1 to 64 characters. Only letters, digits, and underscores (_) are allowed.

Table 5-91 dimensions data structure description

Parameter	Type	Description
name	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 . Start with a letter. Enter 1 to 32 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.
value	String	Specifies the dimension value, for example, an ECS ID. Start with a letter or a digit. Enter 1 to 256 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.

Table 5-92 datapoints data structure description

Parameter	Type	Description
average	Double	Specifies the average value of metric data within a rollup period.
max	Double	Specifies the maximum value of metric data within a rollup period.
min	Double	Specifies the minimum value of metric data within a rollup period.
sum	Double	Specifies the sum of metric data within a rollup period.
variance	Double	Specifies the variance of metric data within a rollup period.
timestamp	Long	Specifies when the metric is collected. It is a UNIX timestamp in milliseconds.

- 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.
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](#).

5.4.4 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.

URI

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

- Parameter description

Table 5-93 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 .

- Parameters that are used to query the host configuration

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 (_).
type	Yes	String	Specifies the 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 .
from	Yes	String	Specifies the start time of the query. The time is a UNIX timestamp and the unit is ms.
to	Yes	String	Specifies the end time of the query. The time is a UNIX timestamp and the unit is ms. from must be earlier than to .
dim	Yes	String	Specifies the dimension. For example, the ECS dimension is instance_id . 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 . Specifies the dimension. A maximum of three dimensions are supported, and the dimensions are numbered from 0 in dim . {i}=key,value format. key cannot exceed 32 characters and value cannot exceed 256 characters. Example: dim.0=instance_id,i-12345

- Example: Query the configuration information about the ECS whose ID is **33328f02-3814-422e-b688-bfdb93d4051** 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-bfdb93d4051&type=instance_host_info&from=1450234543422&to=1450320943422

Request

None

Response

- Response parameters

Table 5-94 Parameter description

Parameter	Type	Description
datapoints	Array of objects	Specifies the configuration list. If the corresponding configuration information does not exist, datapoints is an empty array and is []. For details, see Table 5-95 .

Table 5-95 datapoints data structure description

Parameter	Type	Description
type	String	Specifies the event type, for example, instance_host_info .
timestamp	Long	Specifies when the event is reported. It is a UNIX timestamp and the unit is ms.
value	String	Specifies the host configuration information.

- 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.

URI

GET /V1.0/{project_id}/quotas

- Parameter description

Table 5-96 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 5-97 Response parameters

Parameter	Type	Description
quotas	Object	Specifies the quota list. For details, see Table 5-98 .

Table 5-98 Data structure description of **quotas**

Parameter	Type	Description
resources	Array of objects	Specifies the resource quota list. For details, see Table 5-99 .

Table 5-99 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.

URI

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

- Parameter description

Table 5-100 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 . <ul style="list-style-type: none"> • 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 5-101 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 5-102 .
status	String	Specifies the resource group status, which can be health , unhealth , or no_alarm_rule . <ul style="list-style-type: none"> • 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 5-104 .
enterprise_project_id	String	Specifies the enterprise project associated with the resource group. The default value 0 indicates enterprise project default .

Table 5-102 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 5-103 .

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 5-103 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 5-104 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.

URI

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

- Parameter description

Table 5-105 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 5-106 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 5-107 .

Table 5-107 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 5-108 .

Table 5-108 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 5-109 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 Response

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.

URI

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

- Parameter description

Table 5-110 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 5-111 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 5-112 .

Table 5-112 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 .

Parameter	Type	Mandatory	Description
dimensions	Array of objects	Yes	Specifies one or more resource dimensions. For details, see Table 5-113 .

Table 5-113 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.

URI

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

- Parameter description

Table 5-114 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.

URI

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

- 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_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 . <ul style="list-style-type: none"> 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 5-116 Parameter description

Parameter	Type	Man dator y	Description
resource_groups	Array of objects	No	Specifies information about one or more resource groups. For details, see Table 5-117 .
meta_data	MetaData object	No	Specifies the number of metadata records in the query result. For details, see Table 5-119 .

Table 5-117 resource_groups data structure description

Parameter	Type	Man dator y	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.
type	String	No	Specifies the method for adding resources to a resource group. The value can be EPS (synchronizing resources from enterprise projects), TAG (dynamic tag matching), or Manual (manually adding resources). Minimum length: 0 Maximum length: 32
resources	Array of Resource objects	No	Specifies information about one or more resources. Array length: 0 to 20

Parameter	Type	Mandatory	Description
instance_statistics	InstanceStatistics object	No	Specifies the resource statistics in the resource group. For details, see Table 5-118 .
status	String	No	Specifies the resource group status, which can be health , unhealth , or no_alarm_rule . <ul style="list-style-type: none"> • 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 5-118 instance_statistics data structure description

Parameter	Type	Mandatory	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 5-119 meta_data data structure description

Parameter	Type	Man dato ry	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": []
    }
  ]
}
```

```

},
"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.
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.

URI

POST /V1.0/{project_id}/events

- Parameter description

Table 5-120 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}/events

Request

NOTE

Events with the same **time**, **project_id**, **event_source**, **event_name**, **event_type**, **event_state**, **event_level**, **event_user**, **resource_id** and **resource_name** fields are considered as the same event.

- Request parameters

Table 5-121 Parameter description

Parameter	Type	Mandatory	Description
[Array element]	Array of EventItem objects	Yes	Specifies the event list.

Table 5-122 Parameter description of the **EventItem** field

Parameter	Mandatory	Type	Description
event_name	Yes	String	Specifies the event name. Start with a letter. Enter 1 to 64 characters. Only letters, digits, and underscores (_) are allowed.
event_source	Yes	String	Specifies the event source. 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 (_).
time	Yes	Long	Specifies when the event occurred, which is a UNIX timestamp (ms). NOTE Since there is a latency between the client and the server, the data timestamp to be inserted should be within the period that starts from one hour before the current time plus 20s to 10 minutes after the current time minus 20s. In this way, the timestamp will be inserted to the database without being affected by the latency. For example, if the current time is 2020.01.30 12:00:30, the timestamp inserted must be within the range [2020.01.30 11:00:50, 2020.01.30 12:10:10]. The corresponding UNIX timestamp is [1580353250, 1580357410].
detail	Yes	Detail object	Specifies the event details. For details, see Table 5-123 .

Table 5-123 detail data structure description

Parameter	Mandatory	Type	Description
content	No	String	Specifies the event content. Enter up to 4,096 characters.

Parameter	Mandatory	Type	Description
group_id	No	String	<p>Specifies the resource group the event belongs to.</p> <p>This ID must be an existing resource group ID.</p> <p>To query the group ID, perform the following steps:</p> <ol style="list-style-type: none"> 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.
resource_id	No	String	<p>Specifies the resource ID. Enter up to 128 characters, including letters, digits, underscores (_), hyphens (-), and colon (:).</p> <p>Example: 6a69bf28-ee62-49f3-9785-845dacd799ec</p> <p>To query the resource ID, perform the following steps:</p> <ol style="list-style-type: none"> 1. Log in to the management console. 2. Under Computing, select Elastic Cloud Server. On the Resource Overview page, obtain the resource ID.
resource_name	No	String	<p>Specifies the resource name. Enter up to 128 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).</p>
event_status	No	String	<p>Specifies the event status.</p> <p>The value can be normal, warning, or incident.</p>
event_level	No	String	<p>Specifies the event severity.</p> <p>The value can be Critical, Major, Minor, or Info.</p>
event_user	No	String	<p>Specifies the event user.</p> <p>Enter up to 64 characters, including letters, digits, underscores (_), hyphens (-), slashes (/), and spaces.</p>

Parameter	Mandatory	Type	Description
event_type	No	String	Specifies the event type. Its value can be EVENT.SYS or EVENT.CUSTOM . EVENT.SYS indicates system events that cannot be reported by users. Only custom events can be reported.
dimensions	No	Array of objects	Specifies the event dimension. Currently, a maximum of four dimensions are supported. Resource information is described by dimension. Event alarm rules can be configured by dimension to monitor resources and resource groups. For parameter details, see Table 5-124 .

Table 5-124 dimensions data structure description

Parameter	Type	Mandatory	Description
name	String	Yes	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 .
value	String	Yes	Specifies the dimension value, for example, an ECS ID. The parameter can contain 1 to 256 characters.

- Example request

```
[{
  "event_name": "systemInvaded",
  "event_source": "financial.System",
  "time": 1522121194000,
  "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"
  }
},
{
  "event_name": "systemInvaded",
  "event_source": "financial.System",
  "time": 1522121194020,
```

```

"detail":{
  "content":"The financial system was invaded",
  "group_id":"rg15221211517051YWWkEnVd",
  "resource_id":"1234567890sjgggad",
  "resource_name":"ecs001",
  "event_state":"normal",
  "event_level":"Major",
  "event_user":"xihong",
  "event_type": "EVENT.CUSTOM"
}
}

```

Response

- Response parameters

Table 5-125 Parameter description

Parameter	Type	Description
Array elements	Array of objects	Specifies the event list. For details, see Table 5-126 .

Table 5-126 Response parameters

Parameter	Mandatory	Type	Description
event_id	Yes	String	Specifies the event ID.
event_name	Yes	String	Specifies the event name. Start with a letter. Enter 1 to 64 characters. Only letters, digits, and underscores (_) are allowed.

- Example response

```

[
  {
    "event_id":"evdgiqwgedkkcvhdjcd346",
    "event_name":"systemInvaded"
  },
  {
    "event_id":"evdgiqwgedkkcvhdjcd347",
    "event_name":"systemParalysis"
  }
]

```

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.

URI

GET /V1.0/{project_id}/events

- Parameter description

Table 5-127 Parameter description

Parameter	Type	Mandator y	Description
project_id	String	Yes	Specifies the project ID. For details about how to obtain the project ID, see Obtaining a Project ID .
event_type	String	No	Specifies the event type. Possible types are EVENT.SYS (system event) and EVENT.CUSTOM (custom event).
event_name	String	No	Specifies the event name. The name can be a system event name or a custom event name.

Parameter	Type	Mandatory	Description
from	Integer	No	Specifies the start time of the query. The time is a UNIX timestamp and the unit is ms. Example: 1605952700911
to	Integer	No	Specifies the end time of the query. The time is a UNIX timestamp and the unit is ms. from must be smaller than to . For example, set to to 1606557500911 .
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 events that can be queried at a time. Supported range: 1 to 100 (default)

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

Request

None

Response

- Response parameters

Table 5-128 Parameter description

Parameter	Type	Mandatory	Description
events	Array of Events objects	No	Specifies one or more pieces of event data. For details, see Table 5-129 .
meta_data	MetaData object	No	Specifies the number of metadata records in the query result. For details, see Table 5-130 .

Table 5-129 events field description

Parameter	Type	Mandatory	Description
event_name	String	No	Specifies the event name.
event_type	String	No	Specifies the event type.
event_count	Integer	No	Specifies the number of occurrences of this event within the specified query time range.
latest_occur_time	Long	No	Specifies when the event last occurred.
latest_event_source	String	No	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.

Table 5-130 meta_data data structure description

Parameter	Type	Mandatory	Description
total	Integer	No	Specifies the total number of events.

- Example response

```
{
  "events": [
    {
      "event_name": "rebootServer",
      "event_type": "EVENT.SYS",
      "event_count": 5,
      "latest_occur_time": 1606302400000,
      "latest_event_source": "SYS.ECS"
    },
    {
      "event_name": "deleteVolume",
      "event_type": "EVENT.SYS",
      "event_count": 6,
      "latest_occur_time": 1606300359126,
      "latest_event_source": "SYS.EVS"
    },
    {
      "event_name": "event_001",
      "event_type": "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.

URI

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

- Parameter description

Table 5-131 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 .

Parameter	Type	Mandatory	Description
event_name	String	Yes	Specifies the event name.
event_type	String	Yes	Specifies the event type. The value can be EVENT.SYS (system event) or EVENT.CUSTOM (custom event).
event_source	String	No	Specifies the event name. The name can be a system event name or a custom event name.
event_level	String	No	Specifies the event severity. The value can be Critical , Major , Minor , or Info .
event_user	String	No	Specifies the name of the user who reports the event monitoring data. It can also be a project ID.
event_state	String	No	Specifies the event status. The value can be normal , warning , or incident .
from	Long	No	Specifies the start time of the query. The time is a UNIX timestamp and the unit is ms. Example: 1605952700911
to	Long	No	Specifies the end time of the query. The time is a UNIX timestamp and the unit is ms. The from value must be smaller than the to value.
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}/event/{event_name}

Request

None

Response

- Response parameters

Table 5-132 Parameter description

Parameter	Type	Mandatory	Description
event_name	String	No	Specifies the event name. The name can be a system event name or a custom event name.
event_type	String	No	Specifies the event type. The value can be EVENT.SYS (system event) or EVENT.CUSTOM (custom event).
event_users	Array of strings	No	Specifies the name of the user who reports the event. It can also be a project ID.
event_sources	Array of strings	No	Specifies the event source. For 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.
event_info	Array of objects	No	Specifies details of one or more events. For details, see Table 5-133 .
meta_data	MetaData object	No	Specifies the number of metadata records in the query result. For details, see Table 5-136 .

Table 5-133 event_info data structure description

Parameter	Type	Mandatory	Description
event_name	String	Yes	Specifies the event name. Start with a letter. Enter 1 to 64 characters. Only letters, digits, and underscores (_) are allowed.
event_source	String	No	Specifies the event source in the format of service.item. service and item each must start with a letter and contain 3 to 32 characters, including only letters, digits, and underscores (_).

Parameter	Type	Mandatory	Description
time	Long	Yes	Specifies when the event occurred, which is a UNIX timestamp (ms). Since there is a latency between the client and the server, the data timestamp to be inserted should be within the period that starts from one hour before the current time plus 20s to 10 minutes after the current time minus 20s. In this way, the timestamp will be inserted to the database without being affected by the latency.
detail	Detail object	Yes	Specifies the event details. For details, see Table 5-134 .
event_id	String	No	Specifies the event ID.

Table 5-134 detail data structure description

Parameter	Type	Mandatory	Description
content	String	No	Specifies the event content. Enter up to 4,096 characters.
group_id	String	No	Specifies the resource group the event belongs to. This ID must be an existing resource group ID.
resource_id	String	No	Specifies the resource ID, which can contain a maximum of 128 characters.
resource_name	String	No	Specifies the resource name, which can contain a maximum of 128 characters.
event_state	String	No	Specifies the event status. The value can be normal , warning , or incident .
event_level	String	No	Specifies the event severity. The value can be Critical , Major , Minor , or Info .
event_user	String	No	Specifies the event user. Enter up to 64 characters.

Parameter	Type	Mandatory	Description
event_type	String	No	Specifies the event type. The value can be EVENT.SYS (system event) or EVENT.CUSTOM (custom event).
dimensions	Array of objects	No	Specifies one or more resource dimensions. For details, see Table 5-135 .

Table 5-135 dimensions data structure description

Parameter	Type	Mandatory	Description
name	String	No	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 .
value	String	No	Specifies the dimension value, for example, an ECS ID. Enter 1 to 256 characters.

Table 5-136 meta_data data structure description

Parameter	Type	Mandatory	Description
total	Integer	No	Specifies the total number of events.

- Example response

```
{
  "event_name": "rebootServer",
  "event_type": "EVENT.SYS",
  "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",
  "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",
    "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-
795-4b5f-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",
    "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.
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 an alarm rule (recommended).

URI

POST /v2/{project_id}/alarms

Table 6-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64

Request Parameters

Table 6-2 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	Specifies the MIME type of the 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. Minimum: 1 Maximum: 16384

Table 6-3 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the name of an alarm rule. The name can contain 1 to 128 characters, including only letters, digits, underscores (_), and hyphens (-).
description	No	String	Provides supplementary information about an alarm rule. The description can contain 0 to 256 characters.
namespace	Yes	String	Specifies the namespace of a service. For details about the namespace of each service, see Namespace .
resource_group_id	No	String	Specifies the resource group ID. This parameter is mandatory when the monitoring scope is resource groups.

Parameter	Mandatory	Type	Description
resources	Yes	Array<Array< Dimension >>	Specifies the 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. Array Length: 0 - 1000
policies	No	Array of Policy objects	Specifies the alarm policy. Array Length: 1 - 50
type	Yes	String	Specifies the alarm rule type. 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: <ul style="list-style-type: none"> • EVENT.SYS • EVENT.CUSTOM • DNSHealthCheck • RESOURCE_GROUP • MULTI_INSTANCE • ALL_INSTANCE
alarm_notifications	No	Array of Notification objects	Specifies the action to be triggered by an alarm.
ok_notifications	No	Array of Notification objects	Specifies the action to be triggered after an alarm is cleared.

Parameter	Mandatory	Type	Description
notification_b egin_time	No	String	Specifies the time when the alarm notification was enabled.
notification_e nd_time	No	String	Specifies the time when the alarm notification was disabled.
enterprise_pro ject_id	No	String	Specifies the enterprise project ID.
enabled	Yes	Boolean	Specifies whether to generate alarms when the alarm triggering conditions are met.
notification_e nabled	Yes	Boolean	Specifies whether to enable the alarm notification.
alarm_templa te_id	No	String	Specifies the 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. Array Length: 0 - 20

Table 6-4 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the dimension of a resource. For example, the dimension of an Elastic Cloud Server (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}\$

Parameter	Mandatory	Type	Description
value	No	String	Specifies the 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] _ \.\.)* \^){1,256})\$

Table 6-5 Policy

Parameter	Mandatory	Type	Description
metric_name	Yes	String	Specifies the 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	<p>Specifies the rollup 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.</p> <p>Minimum: 0 Maximum: 86400 Enumeration values:</p> <ul style="list-style-type: none"> • 0 • 1 • 300 • 1200 • 3600 • 14400 • 86400
filter	Yes	String	<p>Specifies the rollup method. The value can be average, min, max, or sum.</p>

Parameter	Mandatory	Type	Description
comparison_operator	Yes	String	Specifies the 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.
unit	No	String	Specifies the metric unit.
count	Yes	Integer	Specifies the number of times that the alarm triggering conditions are met. 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	<p>Specifies the 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.</p> <p>Minimum: 0 Maximum: 86400 Enumeration values:</p> <ul style="list-style-type: none"> • 0 • 300 • 600 • 900 • 1800 • 3600 • 10800 • 21600 • 43200 • 86400
level	No	Integer	<p>Alarm severity, which can be 1 (critical), 2 (major), 3 (minor), or 4 (informational). The default value is 2.</p>

Table 6-6 Notification

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the notification type. notification indicates that notifications are sent through Simple Message Notification (SMN). Regex Pattern: ^(notification autoscaling ecsRecovery contact contactGroup iecAction)\$
notification_list	Yes	Array of strings	Specifies the 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". When type is set to notification , notification_list cannot be left blank. Note: If alarm_action_enabled is set to true , alarm_actions , ok_actions , or both of them must be specified. If alarm_actions and ok_actions coexist, their notification_list values must be the same. Array Length: 0 - 20

Table 6-7 ResourceTag

Parameter	Mandatory	Type	Description
key	Yes	String	Tag key. A tag key can contain up to 128 Unicode characters. Minimum: 1 Maximum: 128 Regex Pattern: ^((?!\\s)(?!_sys_)\\p{L}\\p{Z}\\p{N}_.:+=\\-@]*)?(?!\\s)\$

Parameter	Mandatory	Type	Description
value	Yes	String	Value. Each tag value can contain a maximum of 255 Unicode characters. Minimum: 0 Maximum: 255 Regex Pattern: ^([\p{L}\p{Z}\p{N}_:\./=+\-@]*)\$

Response Parameters

Status code: 201

Table 6-8 Response body parameters

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

Status code: 400

Table 6-9 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-10 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

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",
    "value" : "rdsxxx"
  } ] ],
  "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" : "aCzk8o9dtSQHtiDgb44Eepw"
}
```

Status Codes

Status Code	Description
201	Alarm rule created.
400	Failed to verify parameters.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.1.2 Deleting Alarm Rules in Batches

Function

This API is used to batch delete alarm rules.

URI

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

Table 6-11 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64

Request Parameters

Table 6-12 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	Specifies the user token. Minimum: 1 Maximum: 16384

Table 6-13 Request body parameters

Parameter	Mandatory	Type	Description
alarm_ids	Yes	Array of strings	Specifies the IDs of the alarm rules to be deleted in batches. Array Length: 1 - 10

Response Parameters

Status code: 200

Table 6-14 Response body parameters

Parameter	Type	Description
alarm_ids	Array of strings	Specifies the IDs of the alarm rules that are deleted. Array Length: 1 - 10

Status code: 400

Table 6-15 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-16 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Deleting Alarm Rules in Batches

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

Example Responses

Status code: 200

Alarm rules deleted.

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

Status Codes

Status Code	Description
200	Alarm rules deleted.
400	Failed to verify parameters.
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.

URI

POST /v2/{project_id}/alarms/action

Table 6-17 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64

Request Parameters

Table 6-18 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	Specifies the MIME type of the 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. Minimum: 1 Maximum: 16384

Table 6-19 Request body parameters

Parameter	Mandatory	Type	Description
alarm_ids	Yes	Array of strings	Specifies IDs of alarm rules to be enabled or disabled in batches. Array Length: 1 - 100
alarm_enabled	Yes	Boolean	Specifies whether to generate alarms when the alarm triggering conditions are met.

Response Parameters

Status code: 200

Table 6-20 Response body parameters

Parameter	Type	Description
alarm_ids	Array of strings	Specifies IDs of alarm rules that were enabled or disabled. Array Length: 1 - 100

Status code: 400

Table 6-21 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-22 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

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	Failed to verify parameters.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.1.4 Querying Alarm Rules (Recommended)

Function

This API is used to query alarm rules (recommended).

URI

GET /v2/{project_id}/alarms

Table 6-23 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64

Table 6-24 Query Parameters

Parameter	Mandatory	Type	Description
alarm_id	No	String	Specifies the alarm rule ID. Regex Pattern: <code>^al([0-9A-Za-z]){22}\$</code>
name	No	String	Specifies the name of an alarm rule. The name can contain 1 to 128 characters, including only letters, digits, underscores (_), and hyphens (-). Minimum: 1 Maximum: 128 Regex Pattern: <code>^([\u4E00-\u9FFF] [a-z][A-Z][0-9] _ -)+\$</code>
namespace	No	String	Specifies the namespace of a service. For details about the namespace of each service, see Namespace . Maximum: 32 Regex Pattern: <code>^((([a-z][A-Z]){1}([a-z][A-Z][0-9] _)*\.[a-z][A-Z]){1}([a-z][A-Z][0-9] _)*))\$</code>

Parameter	Mandatory	Type	Description
resource_id	No	String	<p>Specifies the 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 (,). For example, if the monitored resource is an ECS disk, the dimension name disk is placed before the dimension name instance_id in alphabetical order. In this case, the resource ID must be combined as <i>Disk ID,Instance ID</i>.</p> <p>Maximum: 700</p> <p>Regex Pattern: ^([a-z] [A-Z] [0-9] _ - : , \.)+\$</p>
enterprise_project_id	No	String	<p>Specifies the enterprise project ID.</p> <p>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)\$</p>
offset	No	Integer	<p>Specifies the pagination offset.</p> <p>Minimum: 0</p> <p>Maximum: 10000</p> <p>Default: 0</p> <p>Regex Pattern: ^([0] [1-9] [1-9][0-9] [1-9][0-9][0-9] [1-9][0-9][0-9][0-9] 10000)\$</p>
limit	No	Integer	<p>Specifies the number of records that will be displayed on each page.</p> <p>Minimum: 1</p> <p>Maximum: 100</p> <p>Default: 10</p> <p>Regex Pattern: ^([1-9] [1-9][0-9] 100)\$</p>

Request Parameters

Table 6-25 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	Specifies the MIME type of the 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. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-26 Response body parameters

Parameter	Type	Description
alarms	Array of alarms objects	Specifies the alarm rule list. Array Length: 1 - 100
count	Integer	Specifies the total number of alarm rules. Minimum: 0 Maximum: 10000

Table 6-27 alarms

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

Parameter	Type	Description
name	String	Specifies the name of an alarm rule. The name can contain 1 to 128 characters, including only letters, digits, underscores (_), and hyphens (-).
description	String	Provides supplementary information about an alarm rule. The description can contain 0 to 256 characters.
namespace	String	Specifies the namespace of a service. For details about the namespace of each service, see Namespace .
policies	Array of Policy objects	Specifies the alarm policy. Array Length: 1 - 100
resources	Array of ResourcesInListResp objects	Specifies the resource list. Associated resources can be obtained by calling the API for querying resources in an alarm rule. Array Length: 1 - 3000
type	String	Specifies the alarm rule type. 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: <ul style="list-style-type: none"> • EVENT.SYS • EVENT.CUSTOM • DNSHealthCheck • RESOURCE_GROUP • MULTI_INSTANCE • ALL_INSTANCE
enabled	Boolean	Specifies whether to generate alarms when the alarm triggering conditions are met.
notification_enabled	Boolean	Specifies whether to enable the alarm notification.

Parameter	Type	Description
alarm_notifications	Array of Notification objects	Specifies the action to be triggered by an alarm.
ok_notifications	Array of Notification objects	Specifies the action to be triggered after an alarm is cleared.
notification_begin_time	String	Specifies the time when the alarm notification was enabled.
notification_end_time	String	Specifies the time when the alarm notification was disabled.
enterprise_project_id	String	Specifies the enterprise project ID.
alarm_template_id	String	Specifies the 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.

Table 6-28 Policy

Parameter	Type	Description
metric_name	String	Specifies the 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	<p>Specifies the rollup 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.</p> <p>Minimum: 0</p> <p>Maximum: 86400</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • 0 • 1 • 300 • 1200 • 3600 • 14400 • 86400
filter	String	<p>Specifies the rollup method. The value can be average, min, max, or sum.</p>
comparison_operator	String	<p>Specifies the 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.</p>
value	Number	Alarm threshold.
unit	String	Specifies the metric unit.

Parameter	Type	Description
count	Integer	Specifies the number of times that the alarm triggering conditions are met. 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	Integer	Specifies the 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. Minimum: 0 Maximum: 86400 Enumeration values: <ul style="list-style-type: none"> • 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 .

Table 6-29 ResourcesInListResp

Parameter	Type	Description
resource_group_id	String	Specifies the resource group ID. This parameter is available when the monitoring scope is resource groups. Regex Pattern: ^rg([a-z][A-Z][0-9]){2}\$
resource_group_name	String	Specifies the resource group name. This parameter is available when the monitoring scope is resource groups. Minimum: 1 Maximum: 128
dimensions	Array of MetricDimension objects	Specifies the dimension. Array Length: 0 - 10000

Table 6-30 MetricDimension

Parameter	Type	Description
name	String	Specifies the name of a metric dimension. Minimum: 1 Maximum: 32 Regex Pattern: ^([a-z][A-Z]){1}([a-z][A-Z][0-9] _){1,32}\$
value	String	Specifies the value of a metric dimension. Minimum: 0 Maximum: 256 Regex Pattern: ^(((a-z A-Z 0-9){1}(a-z A-Z 0-9 _)*))){0,256}\$

Table 6-31 Notification

Parameter	Type	Description
type	String	Specifies the notification type. notification indicates that notifications are sent through Simple Message Notification (SMN). Regex Pattern: ^(notification autoscaling ecsRecovery contact contactGroup iecAction)\$
notification_list	Array of strings	Specifies the 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". When type is set to notification , notification_list cannot be left blank. Note: If alarm_action_enabled is set to true , alarm_actions , ok_actions , or both of them must be specified. If alarm_actions and ok_actions coexist, their notification_list values must be the same. Array Length: 0 - 20

Status code: 400

Table 6-32 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-33 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Querying 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
} ]
}

```

Status Codes

Status Code	Description
200	Query succeeded.
400	Failed to verify parameters.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.2 Resources in an Alarm Rule

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.

URI

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

Table 6-34 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64
alarm_id	Yes	String	Specifies the alarm rule ID. Regex Pattern: al([a-z] [A-Z] [0-9]){22}\$

Request Parameters

Table 6-35 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	Specifies the MIME type of the 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. Minimum: 1 Maximum: 16384

Table 6-36 Request body parameters

Parameter	Mandatory	Type	Description
resources	Yes	Array<Array< Dimension >>	Specifies the resource information. Array Length: 0 - 1000

Table 6-37 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the dimension of a resource. For example, the dimension of an Elastic Cloud Server (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: <code>^([a-z] [A-Z]){1}([a-z] [A-Z] [0-9] _ -){1,32}\$</code>

Parameter	Mandatory	Type	Description
value	No	String	Specifies the 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] _ \.\.)* *){1,256})\$

Response Parameters

Status code: 400

Table 6-38 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-39 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256

Parameter	Type	Description
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-40 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Batch Adding Resources to an Alarm Rule

```
{
  "resources": [ [ {
    "name": "rds_cluster_id",
    "value": "rds0000000000001"
  } ] ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Resources added.
400	Failed to verify parameters.
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.

URI

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

Table 6-41 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64
alarm_id	Yes	String	Specifies the alarm rule ID. Regex Pattern: al([a-z] [A-Z] [0-9]){22}\$

Request Parameters

Table 6-42 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	Specifies the MIME type of the 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. Minimum: 1 Maximum: 16384

Table 6-43 Request body parameters

Parameter	Mandatory	Type	Description
resources	Yes	Array<Array< Dimension >>	Specifies the resource information. Array Length: 0 - 1000

Table 6-44 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the dimension of a resource. For example, the dimension of an Elastic Cloud Server (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: <code>^([a-z] [A-Z]){1}([a-z] [A-Z] [0-9] _ -){1,32}\$</code>

Parameter	Mandatory	Type	Description
value	No	String	Specifies the 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] _ \.\.)* *){1,256})\$

Response Parameters

Status code: 400

Table 6-45 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-46 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256

Parameter	Type	Description
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-47 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Batch Deleting Resources from an Alarm Rule

```
{
  "resources": [ [ {
    "name": "rds_cluster_id",
    "value": "rds0000000000001"
  } ] ]
}
```

Example Responses

None

Status Codes

Status Code	Description
200	Resources deleted.
400	Failed to verify parameters.
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.

URI

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

Table 6-48 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64
alarm_id	Yes	String	Specifies the alarm rule ID. Regex Pattern: a([a-z] [A-Z] [0-9]){22}\$

Table 6-49 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Specifies the pagination offset. Minimum: 0 Maximum: 10000 Default: 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	Specifies the number of records that will be displayed on each page. Minimum: 1 Maximum: 100 Default: 10 Regex Pattern: ^([1-9] [1-9][0-9] 100)\$

Request Parameters

Table 6-50 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	Specifies the MIME type of the 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. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-51 Response body parameters

Parameter	Type	Description
resources	Array<Array< Dimension >>	Specifies the resource information. Array Length: 0 - 1000
count	Integer	Specifies the total number of resources. Minimum: 0 Maximum: 2147483647

Table 6-52 Dimension

Parameter	Type	Description
name	String	Specifies the dimension of a resource. For example, the dimension of an Elastic Cloud Server (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	String	Specifies the 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]_ -\.)*) *){1,256}\$

Status code: 400

Table 6-53 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256

Parameter	Type	Description
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-54 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

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	Failed to verify parameters.
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 policy.

URI

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

Table 6-55 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64
alarm_id	Yes	String	Specifies the alarm rule ID. Regex Pattern: ^al([0-9A-Za-z]){22}\$

Request Parameters

Table 6-56 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	Specifies the MIME type of the 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. Minimum: 1 Maximum: 16384

Table 6-57 Request body parameters

Parameter	Mandatory	Type	Description
policies	Yes	Array of UpdatePolicy objects	Specifies the policy information. Array Length: 1 - 50

Table 6-58 UpdatePolicy

Parameter	Mandatory	Type	Description
metric_name	Yes	String	Specifies the 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	<p>Specifies the rollup 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.</p> <p>Minimum: 0 Maximum: 86400 Enumeration values:</p> <ul style="list-style-type: none"> • 0 • 1 • 300 • 1200 • 3600 • 14400 • 86400
filter	Yes	String	<p>Specifies the rollup method. The value can be average, min, max, or sum.</p>

Parameter	Mandatory	Type	Description
comparison_operator	Yes	String	Specifies the 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.
unit	No	String	Specifies the metric unit.
type	No	String	Specifies the alarm policy type. This parameter is left blank by default. Minimum: 0 Maximum: 32
count	Yes	Integer	Specifies the number of times that the alarm triggering conditions are met. 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	<p>Specifies the 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.</p> <p>Minimum: 0 Maximum: 86400 Enumeration values:</p> <ul style="list-style-type: none"> • 0 • 300 • 600 • 900 • 1800 • 3600 • 10800 • 21600 • 43200 • 86400
level	No	Integer	<p>Alarm severity, which can be 1 (critical), 2 (major), 3 (minor), or 4 (informational). The default value is 2.</p>

Response Parameters

Status code: 200

Table 6-59 Response body parameters

Parameter	Type	Description
policies	Array of UpdatePolicy objects	Specifies the policy information. Array Length: 1 - 50

Table 6-60 UpdatePolicy

Parameter	Type	Description
metric_name	String	Specifies the 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	Integer	Specifies the rollup 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. Minimum: 0 Maximum: 86400 Enumeration values: <ul style="list-style-type: none"> • 0 • 1 • 300 • 1200 • 3600 • 14400 • 86400

Parameter	Type	Description
filter	String	Specifies the rollup method. The value can be average , min , max , or sum .
comparison_operator	String	Specifies the 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.
unit	String	Specifies the metric unit.
type	String	Specifies the alarm policy type. This parameter is left blank by default. Minimum: 0 Maximum: 32
count	Integer	Specifies the number of times that the alarm triggering conditions are met. 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	Specifies the 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. Minimum: 0 Maximum: 86400 Enumeration values: <ul style="list-style-type: none"> • 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 .

Status code: 400

Table 6-61 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256

Parameter	Type	Description
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-62 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Modifying 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

Alarm policy modified.

```
{
  "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	Alarm policy modified.
400	Failed to verify parameters.
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.

URI

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

Table 6-63 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64
alarm_id	Yes	String	Specifies the alarm rule ID. Regex Pattern: ^al([0-9A-Za-z]){22}\$

Table 6-64 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Specifies the pagination offset. Minimum: 0 Maximum: 10000 Default: 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	Specifies the number of records that will be displayed on each page. Minimum: 1 Maximum: 100 Default: 10 Regex Pattern: ^([1-9] [1-9][0-9] 100)\$

Request Parameters

Table 6-65 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	Specifies the MIME type of the 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. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-66 Response body parameters

Parameter	Type	Description
policies	Array of ListPolicy objects	Specifies the policy information. Array Length: 0 - 100
count	Integer	Specifies total number of policies in an alarm rule. Minimum: 0 Maximum: 100

Table 6-67 ListPolicy

Parameter	Type	Description
metric_name	String	Specifies the 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	Specifies additional information about an alarm policy. This parameter is left blank by default.

Parameter	Type	Description
period	Integer	<p>Specifies the rollup 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.</p> <p>Minimum: 0</p> <p>Maximum: 86400</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • 0 • 1 • 300 • 1200 • 3600 • 14400 • 86400
filter	String	<p>Specifies the rollup method. The value can be average, min, max, or sum.</p>
comparison_operator	String	<p>Specifies the 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.</p>
value	Number	Alarm threshold.
unit	String	Specifies the metric unit.
type	String	<p>Specifies the alarm policy type. This parameter is left blank by default.</p> <p>Minimum: 0</p> <p>Maximum: 32</p>

Parameter	Type	Description
count	Integer	Specifies the number of times that the alarm triggering conditions are met. 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	Integer	Specifies the 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. Minimum: 0 Maximum: 86400 Enumeration values: <ul style="list-style-type: none"> • 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 .

Table 6-68 MetricExtraInfo

Parameter	Type	Description
origin_metric_name	String	Specifies the original metric name. Minimum: 0 Maximum: 64

Parameter	Type	Description
metric_prefix	String	Specifies the metric name prefix. Minimum: 0 Maximum: 8
custom_proc_name	String	Specifies the name of a user process. Minimum: 0 Maximum: 64
metric_type	String	Specifies the metric type. Minimum: 0 Maximum: 16

Status code: 400

Table 6-69 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-70 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256

Parameter	Type	Description
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-71 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Querying 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": [ {
    "metric_name": "disk_device_read_bytes_rate",
    "extra_info": { },
    "period": 1,
    "filter": "average",
    "comparison_operator": ">"
  }
]
```



```

"value" : 75,
"unit" : "byte/s",
"count" : 3,
"type" : "",
"suppress_duration" : 10800,
"level" : 2
}],
"count" : 10
}

```

Status Codes

Status Code	Description
200	Query succeeded.
400	Failed to verify parameters.
404	Alarm rule not found.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.4 Alarm 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.

URI

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

Table 6-72 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64

Parameter	Mandatory	Type	Description
alarm_id	Yes	String	Specifies the alarm rule ID. Regex Pattern: ^al([0-9A-Za-z]){22}\$

Request Parameters

Table 6-73 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	Specifies the MIME type of the 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. Minimum: 1 Maximum: 16384

Table 6-74 Request body parameters

Parameter	Mandatory	Type	Description
notification_enabled	Yes	Boolean	Whether to enable alarm notification. 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	Specifies the action to be triggered by an alarm.
ok_notifications	No	Array of Notification objects	Specifies the action to be triggered after an alarm is cleared.
notification_begin_time	No	String	Specifies the time when the alarm notification was enabled.

Parameter	Mandatory	Type	Description
notification_end_time	No	String	Specifies the time when the alarm notification was disabled.

Table 6-75 Notification

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the notification type. notification indicates that notifications are sent through Simple Message Notification (SMN). Regex Pattern: ^(notification autoscaling ecsRecovery contact contactGroup iecAction)\$
notification_list	Yes	Array of strings	Specifies the 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". When type is set to notification , notification_list cannot be left blank. Note: If alarm_action_enabled is set to true , alarm_actions , ok_actions , or both of them must be specified. If alarm_actions and ok_actions coexist, their notification_list values must be the same. Array Length: 0 - 20

Response Parameters

Status code: 200

Table 6-76 Response body parameters

Parameter	Type	Description
notification_enabled	Boolean	Whether to enable alarm notification.

Parameter	Type	Description
alarm_notifications	Array of Notification objects	Specifies the action to be triggered by an alarm.
ok_notifications	Array of Notification objects	Specifies the action to be triggered after an alarm is cleared.
notification_begin_time	String	Specifies the time when the alarm notification was enabled.
notification_end_time	String	Specifies the time when the alarm notification was disabled.

Table 6-77 Notification

Parameter	Type	Description
type	String	Specifies the notification type. notification indicates that notifications are sent through Simple Message Notification (SMN). Regex Pattern: ^(notification autoscaling ecsRecovery contact contactGroup iecAction)\$
notification_list	Array of strings	Specifies the 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". When type is set to notification , notification_list cannot be left blank. Note: If alarm_action_enabled is set to true , alarm_actions , ok_actions , or both of them must be specified. If alarm_actions and ok_actions coexist, their notification_list values must be the same. Array Length: 0 - 20

Status code: 400

Table 6-78 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-79 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Modifying Alarm Notification Information in an Alarm Rule

```
{
  "notification_enabled" : true,
  "alarm_notifications" : [ {
    "type" : "",
    "notification_list" : [ ]
  } ],
  "ok_notifications" : [ {
    "type" : "",
```

```

"notification_list" : [ ]
}],
"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	Failed to verify parameters.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.5 Alarm Records

6.5.1 Querying Alarm Records

Function

This API is used to query alarm records.

URI

GET /v2/{project_id}/alarm-histories

Table 6-80 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>

Table 6-81 Query Parameters

Parameter	Mandatory	Type	Description
alarm_id	No	String	Specifies an alarm ID, which starts with al and is followed by 22 characters, including letters and digits. Minimum: 24 Maximum: 24
record_id	No	String	Alarm record ID, which starts with ah and is followed by 22 characters, including letters and digits. Minimum: 24 Maximum: 24
name	No	String	Specifies the alarm rule name. Minimum: 0 Maximum: 128
alarm_type	No	String	Alarm type. The value can be event (querying event alarms) or metric (querying metric alarms). Enumeration values: <ul style="list-style-type: none"> • event • metric
status	No	String	Specifies the alarm rule status. The value can be ok , alarm , or invalid . Minimum: 0 Maximum: 64 Regex Pattern: <code>^(ok alarm invalid)\$</code>

Parameter	Mandatory	Type	Description
level	No	Integer	Specifies the alarm severity, which can be 1 (critical), 2 (major), 3 (minor), or 4 (informational). Minimum: 1 Maximum: 4
namespace	No	String	Specifies the namespace of a service. For details about the namespace of each service, see Namespace . Minimum: 3 Maximum: 32
resource_id	No	String	Specifies the 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 (,). Minimum: 0 Maximum: 2048
from	No	String	Specifies the start time for querying alarm records, for example, 2022-02-10T10:05:46+08:00 . Minimum: 0 Maximum: 64
to	No	String	Specifies the end time for querying alarm records, for example, 2022-02-10T10:05:47+08:00 . Minimum: 0 Maximum: 64
offset	No	Integer	Specifies the pagination offset. Minimum: 0 Maximum: 999 Default: 0 Regex Pattern: <code>^(0 [1-9] [1-9][0-9])\$</code>

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the number of records that will be displayed on each page. Minimum: 1 Maximum: 100 Default: 100 Regex Pattern: ^([1-9] [1-9][0-9] 100)\$
order_by	No	String	Keyword for sorting alarms. 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). update_time is used by default. Enumeration values: <ul style="list-style-type: none"> • first_alarm_time • update_time • alarm_level • record_id

Request Parameters

Table 6-82 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-83 Response body parameters

Parameter	Type	Description
alarm_histories	Array of AlarmHistoryItemV2 objects	Specifies the alarm records. Array Length: 0 - 100
count	Integer	Specifies the total number of alarm records. Minimum: 0 Maximum: 2147483647

Table 6-84 AlarmHistoryItemV2

Parameter	Type	Description
record_id	String	Specifies the alarm record ID. Minimum: 24 Maximum: 24
alarm_id	String	Specifies the alarm rule ID, for example, al1603131199286dzxpqK3Ez . Minimum: 24 Maximum: 24
name	String	Specifies the alarm rule name, for example, alarm-test01 . Minimum: 1 Maximum: 128
status	String	Specifies the status of an alarm record. The value can be ok , alarm , or invalid . Enumeration values: <ul style="list-style-type: none"> • ok • alarm • invalid

Parameter	Type	Description
level	Integer	Specifies the alarm severity of alarm records. The value can be 1 (critical), 2 (major), 3 (minor), or 4 (informational). Enumeration values: <ul style="list-style-type: none"> • 1 • 2 • 3 • 4
type	String	Specifies the alarm rule type. 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: <ul style="list-style-type: none"> • EVENT.SYS • EVENT.CUSTOM • DNSHealthCheck • RESOURCE_GROUP • MULTI_INSTANCE • ALL_INSTANCE
action_enabled	Boolean	Specifies whether to send a notification. The value can be true or false .
begin_time	String	Specifies when an alarm record is generated (UTC time).
end_time	String	Specifies when an alarm record becomes invalid (UTC time).
first_alarm_time	String	UTC time when the alarm was generated for the first time.
last_alarm_time	String	UTC time when the alarm was generated for the last time.
alarm_recovery_time	String	UTC time when the alarm was cleared.

Parameter	Type	Description
metric	Metric object	Specifies the metric information.
condition	AlarmCondition object	Specifies the conditions for triggering an alarm.
additional_info	AdditionalInfo object	Specifies the additional field of an alarm record, which applies only to alarm records generated in event monitoring scenarios.
alarm_actions	Array of Notification objects	Action to be triggered by an alarm. The structure is as follows: {"type": "notification", "notification_list": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"] }. type can be notification (a notification action), autoscaling (a scaling action), or notification_list (when the alarm rule status changes, Cloud Eye will notify users in the notification list). Array Length: 0 - 10
ok_actions	Array of Notification objects	Action to be triggered after an alarm is cleared. The structure is as follows: {"type": "notification", "notification_list": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"] }. type can be notification or notification_list . notification_list indicates that when the alarm rule status changes, Cloud Eye will notify users in the notification list. ' Array Length: 0 - 10
data_points	Array of DataPointInfo objects	Specifies the time when the resource monitoring data is reported and the monitoring data in the alarm record. Array Length: 0 - 2147483647

Table 6-85 Metric

Parameter	Type	Description
namespace	String	Specifies the namespace of a service. For details about the namespace of each service, see Namespace . Minimum: 3 Maximum: 32

Parameter	Type	Description
metric_name	String	Specifies the 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 . Minimum: 1 Maximum: 64
dimensions	Array of Dimension objects	Specifies the metric dimension. A maximum of four dimensions can be added. Array Length: 0 - 4

Table 6-86 Dimension

Parameter	Type	Description
name	String	Specifies the dimension of a resource. For example, the dimension of an Elastic Cloud Server (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	String	Specifies the 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] _ \.)*)\ *)\{1,256\}\$

Table 6-87 AlarmCondition

Parameter	Type	Description
period	Integer	<p>Specifies the rollup 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.</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • 0 • 1 • 300 • 1200 • 3600 • 14400 • 86400
filter	String	<p>Specifies the rollup method. The value can be average, min, max, or sum.</p> <p>Minimum: 1</p> <p>Maximum: 15</p> <p>Regex Pattern: <code>^(average min max sum)\$</code></p>
comparison_operator	String	<p>Specifies the 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.</p> <p>Minimum: 1</p> <p>Maximum: 10</p> <p>Regex Pattern: <code>^(> < >= <= = != cycle_decrease cycle_increase cycle_wave)\$</code></p>

Parameter	Type	Description
value	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 Elastic Cloud Server (ECS) cpu_util to 80 . Minimum: 0 Maximum: 1.174271E108
unit	String	Specifies the data unit. Enter up to 32 characters. Minimum: 0 Maximum: 32
count	Integer	Specifies the number of times that the alarm triggering conditions are met. Minimum: 1 Maximum: 180
suppress_duration	Integer	Specifies the 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. Enumeration values: <ul style="list-style-type: none"> • 0 • 300 • 600 • 900 • 1800 • 3600 • 10800 • 21600 • 43200 Regex Pattern: <code>^(0 300 600 900 1800 3600 10800 21600 43200 86400)\$</code>

Table 6-88 AdditionalInfo

Parameter	Type	Description
resource_id	String	Specifies the resource ID corresponding to the alarm record, for example, 22d98f6c-16d2-4c2d-b424-50e79d82838f . Minimum: 0 Maximum: 128
resource_name	String	Specifies the resource name corresponding to the alarm record, for example, ECS-Test01 . Minimum: 0 Maximum: 128
event_id	String	Specifies the ID of the event in the alarm record, for example, ev16031292300990kKN8p17J . Minimum: 24 Maximum: 24

Table 6-89 Notification

Parameter	Type	Description
type	String	Specifies the notification type. notification indicates that notifications are sent through Simple Message Notification (SMN). Regex Pattern: <code>^(notification autoscaling ecsRecovery contact contactGroup iecAction)\$</code>
notification_list	Array of strings	Specifies the 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". When type is set to notification , notification_list cannot be left blank. Note: If alarm_action_enabled is set to true , alarm_actions , ok_actions , or both of them must be specified. If alarm_actions and ok_actions coexist, their notification_list values must be the same. Array Length: 0 - 20

Table 6-90 DataPointInfo

Parameter	Type	Description
time	String	Specifies the UTC time when the resource monitoring data of the alarm record is reported. Minimum: 1 Maximum: 64
value	Double	Specifies the resource monitoring data of the alarm record at the time point, for example, 7.019 . Minimum: 0 Maximum: 1.7976931348623157E308

Status code: 400

Table 6-91 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-92 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Querying 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",
    "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	Failed to verify parameters.
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.

URI

POST /v2/{project_id}/alarm-templates

Table 6-93 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64

Request Parameters

Table 6-94 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the tenant token. Minimum: 1 Maximum: 16384

Table 6-95 Request body parameters

Parameter	Mandatory	Type	Description
template_name	Yes	String	Specifies the 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	Specifies the type of a custom alarm template. 0 indicates an alarm template for metrics. 2 indicates an alarm template for events. Enumeration values: <ul style="list-style-type: none"> • 0 • 2
template_description	No	String	Provides 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	Specifies alarm policies in an alarm template. Array Length: 1 - 50

Table 6-96 Policies

Parameter	Mandatory	Type	Description
namespace	Yes	String	Specifies the namespace of a service. For details about the namespace of each service, see Namespace .
dimension_name	No	String	Specifies the 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	Specifies the metric name.
period	Yes	Integer	Specifies the interval (seconds) for checking whether the alarm rule conditions are met. Enumeration values: <ul style="list-style-type: none"> • 0 • 1 • 300 • 1200 • 3600 • 14400 • 86400
filter	Yes	String	Specifies the data rollup method. Regex Pattern: ^(average variance min max sum)\$

Parameter	Mandatory	Type	Description
comparison_operator	Yes	String	Specifies the 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	Specifies the alarm threshold. Minimum: 0 Maximum: 1.7976931348623156E108
unit	No	String	Specifies the data unit. The value can contain up to 32 characters. Minimum: 0 Maximum: 32
count	Yes	Integer	Specifies the 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). The default value is 2 .

Parameter	Mandatory	Type	Description
suppress_duration	Yes	Integer	Specifies the alarm suppression period, in seconds. When the period is 0 , only one alarm is generated. Enumeration values: <ul style="list-style-type: none"> • 0 • 300 • 600 • 900 • 1800 • 3600 • 10800 • 21600 • 43200 • 86400

Response Parameters

Status code: 201

Table 6-97 Response body parameters

Parameter	Type	Description
template_id	String	Specifies the 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 6-98 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256

Parameter	Type	Description
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-99 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-100 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256

Parameter	Type	Description
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-101 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

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	Failed to verify parameters.
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.

URI

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

Table 6-102 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64

Request Parameters

Table 6-103 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the tenant token. Minimum: 1 Maximum: 16384

Table 6-104 Request body parameters

Parameter	Mandatory	Type	Description
template_ids	Yes	Array of strings	Specifies 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. Array Length: 1 - 100
delete_associate_alarm	Yes	Boolean	Specifies 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 6-105 Response body parameters

Parameter	Type	Description
template_ids	Array of strings	Specifies IDs of alarm templates that were deleted successfully. Array Length: 1 - 100

Status code: 400

Table 6-106 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-107 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service codes when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-108 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-109 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Deleting custom alarm templates in batches

```
{
  "template_ids" : [ "at1628592157541dB1kIWgY6" ],
  "delete_associate_alarm" : false
}
```

Example Responses

Status code: 200

Specifies IDs of alarm templates that were successfully deleted.

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

Status Codes

Status Code	Description
200	Specifies IDs of alarm templates that were successfully deleted.
400	Failed to verify parameters.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.6.3 Modifying a Custom Alarm Template

Function

This API is used to modify a custom alarm template.

URI

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

Table 6-110 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64
template_id	Yes	String	Specifies the ID of an alarm template. Minimum: 2 Maximum: 64

Request Parameters

Table 6-111 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the tenant token. Minimum: 1 Maximum: 16384

Table 6-112 Request body parameters

Parameter	Mandatory	Type	Description
template_name	Yes	String	Specifies the 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. Enumeration values: <ul style="list-style-type: none"> • 0 • 2
template_description	No	String	Provides 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	Specifies alarm policies in an alarm template. Array Length: 1 - 50

Table 6-113 Policies

Parameter	Mandatory	Type	Description
namespace	Yes	String	Specifies the namespace of a service. For details about the namespace of each service, see Namespace .
dimension_name	No	String	Specifies the 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	Specifies the metric name.
period	Yes	Integer	Specifies the interval (seconds) for checking whether the alarm rule conditions are met. Enumeration values: <ul style="list-style-type: none"> • 0 • 1 • 300 • 1200 • 3600 • 14400 • 86400
filter	Yes	String	Specifies the data rollup method. Regex Pattern: ^(average variance min max sum)\$

Parameter	Mandatory	Type	Description
comparison_operator	Yes	String	Specifies the 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	Specifies the alarm threshold. Minimum: 0 Maximum: 1.7976931348623156E108
unit	No	String	Specifies the data unit. The value can contain up to 32 characters. Minimum: 0 Maximum: 32
count	Yes	Integer	Specifies the 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). The default value is 2 .

Parameter	Mandatory	Type	Description
suppress_duration	Yes	Integer	Specifies the alarm suppression period, in seconds. When the period is 0 , only one alarm is generated. Enumeration values: <ul style="list-style-type: none"> • 0 • 300 • 600 • 900 • 1800 • 3600 • 10800 • 21600 • 43200 • 86400

Response Parameters

Status code: 400

Table 6-114 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-115 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-116 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-117 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-118 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

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	Failed to verify parameters.
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 alarm templates.

URI

GET /v2/{project_id}/alarm-templates

Table 6-119 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64

Table 6-120 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Specifies the start position for pagination query, indicating the sequence number of the data record where the query starts. The default value is 0 . Minimum: 0 Maximum: 10000
limit	No	Integer	Specifies the maximum number of query results. The value ranges from 1 to 100 (default). Minimum: 1 Maximum: 100
namespace	No	String	Specifies the namespace of a service. For details about the namespace of each service, see Namespace . Minimum: 3 Maximum: 32 Regex Pattern: <code>^([a-z] [A-Z]){1}([a-z] [A-Z] [0-9] _)*\.[a-z] [A-Z]{1}([a-z] [A-Z] [0-9] _)*\$</code>
dim_name	No	String	Specifies the 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. Minimum: 1 Maximum: 131 Regex Pattern: <code>^([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}\$</code>

Parameter	Mandatory	Type	Description
template_type	No	String	Specifies the 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: <ul style="list-style-type: none"> • system • custom • system_event • custom_event • system_custom_event
template_name	No	String	Specifies the 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. Minimum: 1 Maximum: 128 Regex Pattern: ^([\u4E00-\u9FFF] [a-z][A-Z][0-9]_ - \(\) \.\ s)+\$

Request Parameters

Table 6-121 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the tenant token. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-122 Response body parameters

Parameter	Type	Description
alarm_templates	Array of AlarmTemplates objects	Specifies the alarm template list. Array Length: 0 - 100
count	Integer	Specifies the total number of alarm templates. Minimum: 0 Maximum: 9999999

Table 6-123 AlarmTemplates

Parameter	Type	Description
template_id	String	Specifies the 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	Specifies the 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	Specifies the type of an alarm template. custom indicates custom alarm templates, and system indicates default alarm templates. Enumeration values: <ul style="list-style-type: none"> • system • custom
create_time	String	Specifies the time when an alarm template was created.
template_description	String	Provides supplementary information about an alarm template. The description can contain 0 to 256 characters and is left blank by default.

Status code: 400

Table 6-124 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-125 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-126 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-127 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

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	Failed to verify parameters.
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.

URI

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

Table 6-128 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64

Parameter	Mandatory	Type	Description
template_id	Yes	String	Specifies the ID of an alarm template. The ID starts with at and is followed by up to 64 characters, including letters and digits. Minimum: 2 Maximum: 64

Request Parameters

Table 6-129 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the tenant token. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-130 Response body parameters

Parameter	Type	Description
template_id	String	Specifies the 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	Specifies the 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	Specifies the type of an alarm template. custom indicates custom alarm templates, and system indicates default alarm templates. Enumeration values: <ul style="list-style-type: none"> • system • custom

Parameter	Type	Description
create_time	String	Specifies the time when an alarm template was created.
template_description	String	Provides supplementary information about an alarm template. The description can contain 0 to 256 characters and is left blank by default.
policies	Array of GetPolicies objects	Specifies alarm policies in an alarm template. Array Length: 1 - 50

Table 6-131 GetPolicies

Parameter	Type	Description
namespace	String	Specifies the namespace of a service. For details about the namespace of each service, see Namespace .
dimension_name	String	Specifies the 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	Specifies the metric name.
period	Integer	Specifies the interval (seconds) for checking whether the alarm rule conditions are met. Enumeration values: <ul style="list-style-type: none"> • 0 • 1 • 300 • 1200 • 3600 • 14400 • 86400
filter	String	Specifies the data rollup method. Regex Pattern: ^(average variance min max sum)\$

Parameter	Type	Description
comparison_operator	String	Specifies the 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	Specifies the alarm threshold. Minimum: 0 Maximum: 2.34854258277383E108
unit	String	Specifies the data unit. The value can contain up to 32 characters. Minimum: 0 Maximum: 32
count	Integer	Specifies the 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). The default value is 2 .

Parameter	Type	Description
suppress_duration	Integer	Specifies the alarm suppression period, in seconds. When the period is 0 , only one alarm is generated. Enumeration values: <ul style="list-style-type: none"> • 0 • 300 • 600 • 900 • 1800 • 3600 • 10800 • 21600 • 43200 • 86400

Status code: 400

Table 6-132 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-133 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-134 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-135 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-136 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

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,
    "unit" : "bit/s",
    "count" : 2,
    "alarm_level" : 2,
    "suppress_duration" : 300
  } ]
}
```

Status Codes

Status Code	Description
200	OK
400	Failed to verify parameters.
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 an alarm template.

URI

GET /v2/{project_id}/alarm-templates/{template_id}/association-alarms

Table 6-137 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64
template_id	Yes	String	Specifies the ID of an alarm template. The ID starts with at and is followed by up to 64 characters, including letters and digits. Minimum: 2 Maximum: 64

Table 6-138 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Specifies the start position for pagination query, indicating the sequence number of the data record where the query starts. The default value is 0 . Minimum: 0 Maximum: 10000
limit	No	Integer	Specifies the maximum number of query results. The value ranges from 1 to 100 (default). Minimum: 1 Maximum: 100

Request Parameters

Table 6-139 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the tenant token. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-140 Response body parameters

Parameter	Type	Description
alarms	Array of alarms objects	Specifies the alarm rule list. Array Length: 0 - 100
count	Integer	Specifies the total number of alarm rules. Minimum: 0 Maximum: 1000

Table 6-141 alarms

Parameter	Type	Description
alarm_id	String	Specifies the alarm rule ID. Regex Pattern: <code>^al{0-9A-Za-z}{22}\$</code>
name	String	Specifies the alarm rule name. Minimum: 1 Maximum: 128 Regex Pattern: <code>^([\u4E00-\u9FFF] [a-z][A-Z][0-9] _ -)+\$</code>
description	String	Provides supplementary information about an alarm rule. Minimum: 0 Maximum: 256

Status code: 400

Table 6-142 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256

Parameter	Type	Description
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-143 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-144 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256

Parameter	Type	Description
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-145 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Querying 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": "Specifies the alarm rule list."
  } ],
  "count": 100
}
```

Status Codes

Status Code	Description
200	OK
400	Failed to verify parameters.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.8 Resource Groups

6.8.1 This API is used to create a resource group (recommended).

Function

This API is used to create a resource group (recommended).

URI

POST /v2/{project_id}/resource-groups

Table 6-146 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64

Request Parameters

Table 6-147 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the tenant token. Minimum: 1 Maximum: 16384

Table 6-148 Request body parameters

Parameter	Mandatory	Type	Description
group_name	Yes	String	Specifies the resource group name. The value can contain up to 128 characters, including letters, digits, hyphens (-), and underscores (_). Minimum: 1 Maximum: 128 Regex Pattern: ^([\u4E00-\u9FFF] [a-z][A-Z][0-9] _)+\$
enterprise_project_id	No	String	Specifies the ID of the enterprise project to which a resource group belongs. 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	Specifies the method for adding resources to a resource group. The value can only be EPS (synchronizing resources from enterprise projects) or TAG (dynamic tag matching). If this parameter is not specified, resources are manually added. Regex Pattern: ^(EPS TAG Manual COMB)\$
tags	No	Array of ResourceGroupTagRelation objects	Specifies the associated tag during dynamic tag matching. This parameter is mandatory when type is set to TAG . Array Length: 1 - 10

Parameter	Mandatory	Type	Description
association_e p_ids	No	Array of strings	Specifies the ID of the enterprise project from which resources in the resource group come. This parameter is mandatory when type is set to EPS . Array Length: 1 - 10

Table 6-149 ResourceGroupTagRelation

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. Minimum: 1 Maximum: 36
value	No	String	Specifies the tag value. Minimum: 1 Maximum: 42

Response Parameters

Status code: 200

Table 6-150 Response body parameters

Parameter	Type	Description
group_id	String	Specifies the resource group ID, which starts with rg and is followed by 22 characters, including letters and digits.

Status code: 400

Table 6-151 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256

Parameter	Type	Description
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-152 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-153 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256

Parameter	Type	Description
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-154 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

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	Failed to verify parameters.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.8.2 Batch Deleting Resource Groups

Function

This API is used to batch delete resource groups.

URI

POST /v2/{project_id}/resource-groups/batch-delete

Table 6-155 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64

Request Parameters

Table 6-156 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the tenant token. Minimum: 1 Maximum: 16384

Table 6-157 Request body parameters

Parameter	Mandatory	Type	Description
group_ids	Yes	Array of strings	Specifies IDs of resource groups to be deleted in batches. Array Length: 1 - 100

Response Parameters

Status code: 200

Table 6-158 Response body parameters

Parameter	Type	Description
group_ids	Array of strings	Specifies IDs of resource groups that were successfully deleted. Array Length: 1 - 100

Status code: 400

Table 6-159 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-160 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-161 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-162 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Batch deleting resource groups

```
{
  "group_ids" : [ "rg0123456789xxxx" ]
}
```

Example Responses

Status code: 200

Specifies IDs of resource groups that were successfully deleted.

```
{
  "group_ids" : [ "rg0123456789xxxx" ]
}
```

Status Codes

Status Code	Description
200	Specifies IDs of resource groups that were successfully deleted.
400	Failed to verify parameters.
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.

URI

PUT /v2/{project_id}/resource-groups/{group_id}

Table 6-163 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64
group_id	Yes	String	Specifies the resource group ID, which starts with rg and is followed by 22 characters, including letters and digits. Minimum: 2 Maximum: 24

Request Parameters

Table 6-164 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the tenant token. Minimum: 1 Maximum: 16384

Table 6-165 Request body parameters

Parameter	Mandatory	Type	Description
group_name	Yes	String	Specifies the resource group name. The value can contain up to 128 characters, including letters, digits, hyphens (-), and underscores (_). Minimum: 1 Maximum: 128
tags	No	Array of ResourceGroupTagRelation objects	Specifies the associated tag during dynamic tag matching. This parameter must be specified when type is set to TAG . Array Length: 1 - 10

Table 6-166 ResourceGroupTagRelation

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. Minimum: 1 Maximum: 36
value	No	String	Specifies the tag value. Minimum: 1 Maximum: 42

Response Parameters

Status code: **400**

Table 6-167 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256

Parameter	Type	Description
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-168 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-169 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256

Parameter	Type	Description
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-170 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-171 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Modifying 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	Failed to verify parameters.
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.

URI

GET /v2/{project_id}/resource-groups/{group_id}

Table 6-172 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64
group_id	Yes	String	Specifies the resource group ID, which starts with rg and is followed by 22 characters, including letters and digits. Minimum: 2 Maximum: 24

Request Parameters

Table 6-173 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the tenant token. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-174 Response body parameters

Parameter	Type	Description
group_name	String	Specifies the 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	Specifies the resource group ID, which starts with rg and is followed by 22 characters, including letters and digits. Minimum: 2 Maximum: 24
create_time	String	Specifies the time when a resource group was created.

Parameter	Type	Description
enterprise_project_id	String	Specifies the ID of the enterprise project to which a resource group belongs. 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	Specifies the method for adding resources to a resource group. The value can only be EPS (synchronizing resources from enterprise projects), TAG (dynamic tag matching), or Manual (manually adding resources). Enumeration values: <ul style="list-style-type: none"> • EPS • TAG • Manual
association_ep_ids	Array of strings	Specifies the ID of the enterprise project from which resources in the resource group come. This parameter is mandatory when type is set to EPS . Array Length: 1 - 1
tags	Array of ResourceGroupTagRelation objects	Specifies the associated tag during dynamic tag matching. This parameter must be specified when type is set to TAG . Array Length: 1 - 10

Table 6-175 ResourceGroupTagRelation

Parameter	Type	Description
key	String	Specifies the tag key. Minimum: 1 Maximum: 36
value	String	Specifies the tag value. Minimum: 1 Maximum: 42

Status code: 400

Table 6-176 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-177 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-178 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-179 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-180 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Querying 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	Failed to verify parameters.
401	Not authenticated.

Status Code	Description
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.

URI

GET /v2/{project_id}/resource-groups

Table 6-181 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64

Table 6-182 Query Parameters

Parameter	Mandatory	Type	Description
enterprise_project_id	No	String	Specifies the ID of the enterprise project to which a resource group belongs. 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	Specifies the resource group name. Fuzzy search is supported. Minimum: 1 Maximum: 128

Parameter	Mandatory	Type	Description
group_id	No	String	Specifies the resource group ID, which starts with rg and is followed by 22 characters, including letters and digits. Minimum: 2 Maximum: 24
offset	No	Integer	Specifies the start position for pagination query, indicating the sequence number of the data record where the query starts. The default value is 0 . Minimum: 0 Maximum: 10000
limit	No	Integer	Specifies the number of items on each page during pagination query. The value ranges from 1 to 100 (default). Minimum: 1 Maximum: 100
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), or COMB (automatically adding resources – match by multiple criteria). If this parameter is not specified, all resource groups are queried. Enumeration values: <ul style="list-style-type: none"> • EPS • TAG • Manual • COMB

Parameter	Mandatory	Type	Description
origin_flag	No	String	Specifies the source ID. The value can only be resourcegroup or monitoroverview . If this parameter is not specified, resourcegroup is used by default. Enumeration values: <ul style="list-style-type: none"> • resourcegroup • monitoroverview

Request Parameters

Table 6-183 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the tenant token. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-184 Response body parameters

Parameter	Type	Description
count	Integer	Specifies the total number of resource groups. Minimum: 0 Maximum: 1000
resource_groups	Array of OneResourceGroupResp objects	Specifies the resource group list. Array Length: 0 - 100

Table 6-185 OneResourceGroupResp

Parameter	Type	Description
group_name	String	Specifies the 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	Specifies the resource group ID, which starts with rg and is followed by 22 characters, including letters and digits. Minimum: 2 Maximum: 24
create_time	String	Specifies the time when a resource group was created.
enterprise_project_id	String	Specifies the ID of the enterprise project to which a resource group belongs. 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	Specifies the method for adding resources to a resource group. The value can only be EPS (synchronizing resources from enterprise projects), TAG (dynamic tag matching), or Manual (manually adding resources). Enumeration values: <ul style="list-style-type: none"> • EPS • TAG • Manual

Status code: 400

Table 6-186 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256

Parameter	Type	Description
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-187 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-188 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256

Parameter	Type	Description
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-189 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Querying 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	Failed to verify parameters.
401	Not authenticated.
403	Authentication failed.
500	Internal system 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**.

URI

POST /v2/{project_id}/resource-groups/{group_id}/resources/batch-create

Table 6-190 Path Parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	Specifies the resource group ID, which starts with rg and is followed by 22 characters, including letters and digits. Minimum: 2 Maximum: 24

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64

Request Parameters

Table 6-191 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Table 6-192 Request body parameters

Parameter	Mandatory	Type	Description
resources	Yes	Array of Resource objects	Specifies the resource information. Array Length: 1 - 1000

Table 6-193 Resource

Parameter	Mandatory	Type	Description
namespace	Yes	String	Specifies the namespace of a service. For details about the namespace of each service, see Namespace .
dimensions	Yes	Array of Dimension objects	Specifies the resource dimension information. Array Length: 1 - 4

Table 6-194 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the 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 Services Interconnected with Cloud Eye . Regex Pattern: ^([a-z] [A-Z]){1}([a-z] [A-Z] [0-9] _ -){1,32}\$
value	Yes	String	Specifies the 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] _ \.)*)\)*{1,256}\$

Response Parameters

Status code: 200

Table 6-195 Response body parameters

Parameter	Type	Description
succeed_count	Integer	Specifies the number of resources that were successfully added. Minimum: 0 Maximum: 1000

Status code: 400

Table 6-196 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-197 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-198 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Batch Adding Resources to a Resource Group Whose **type** Is **Manual**

```
{
  "resources" : [ {
    "namespace" : "SYS.ECS",
    "dimensions" : [ {
      "name" : "instance_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	Failed to verify parameters.
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**.

URI

POST /v2/{project_id}/resource-groups/{group_id}/resources/batch-delete

Table 6-199 Path Parameters

Parameter	Mandatory	Type	Description
group_id	Yes	String	Specifies the resource group ID, which starts with rg and is followed by 22 characters, including letters and digits. Minimum: 2 Maximum: 24
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64

Request Parameters

Table 6-200 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Table 6-201 Request body parameters

Parameter	Mandatory	Type	Description
resources	Yes	Array of Resource objects	Specifies the resource information. Array Length: 1 - 1000

Table 6-202 Resource

Parameter	Mandatory	Type	Description
namespace	Yes	String	Specifies the namespace of a service. For details about the namespace of each service, see Namespace .
dimensions	Yes	Array of Dimension objects	Specifies the resource dimension information. Array Length: 1 - 4

Table 6-203 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the 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 Services Interconnected with Cloud Eye . Regex Pattern: ^([a-z] [A-Z]){1}([a-z] [A-Z] [0-9] _ -){1,32}\$
value	Yes	String	Specifies the 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] _ \.\.)* *){1,256})\$

Response Parameters

Status code: 200

Table 6-204 Response body parameters

Parameter	Type	Description
succeed_count	Integer	Specifies the number of resources that were successfully deleted. Minimum: 0 Maximum: 1000

Status code: 400

Table 6-205 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-206 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256

Parameter	Type	Description
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-207 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Batch Deleting Resources from a Resource Group Whose **type** is **Manual**

```
{
  "resources" : [ {
    "namespace" : "SYS.ECS",
    "dimensions" : [ {
      "name" : "instance_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	Failed to verify parameters.
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 and a specified service type in a resource group.

URI

GET /v2/{project_id}/resource-groups/{group_id}/services/{service}/resources

Table 6-208 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64
group_id	Yes	String	Specifies the resource group ID, which starts with rg and is followed by 22 characters, including letters and digits. Minimum: 2 Maximum: 24
service	Yes	String	Specifies the service type, for example, SYS.ECS . Minimum: 3 Maximum: 32

Table 6-209 Query Parameters

Parameter	Mandatory	Type	Description
dim_name	No	String	Specifies the resource dimension name. Separate multiple dimensions with commas (,) in alphabetical order. Minimum: 1 Maximum: 131
limit	No	String	Specifies the number of items on each page during pagination query. The value ranges from 1 to 100 (default). Minimum: 1 Maximum: 100
offset	No	Integer	Specifies the start position for pagination query, indicating the sequence number of the data record where the query starts. The default value is 0 . Minimum: 0 Maximum: 10000
status	No	String	Specifies the 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: <ul style="list-style-type: none"> • health • unhealthy • no_alarm_rule

Parameter	Mandatory	Type	Description
dim_value	No	String	Specifies the resource dimension value. Fuzzy match is not supported. If a resource has multiple dimensions, you can specify one of them. Minimum: 1 Maximum: 1027
tag	No	String	Resource tag. The format is [key]:**[value] . Example: ssss:1111 . Minimum: 0 Maximum: 500
extend_relation_id	No	String	Enterprise project ID. Minimum: 0 Maximum: 128

Request Parameters

Table 6-210 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	Specifies the tenant token. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-211 Response body parameters

Parameter	Type	Description
count	Integer	Specifies the total number of resources. Minimum: 0 Maximum: 10000

Parameter	Type	Description
resources	Array of GetResourceGroupResources objects	Specifies the resource list in a resource group. Array Length: 0 - 100

Table 6-212 GetResourceGroupResources

Parameter	Type	Description
status	String	Specifies the resource health status. 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 : The resource is not associated with any alarm rule. Enumeration values: <ul style="list-style-type: none"> • health • unhealthy • no_alarm_rule
dimensions	Array of Dimension objects	Specifies the resource dimension information. Array Length: 1 - 4

Table 6-213 Dimension

Parameter	Type	Description
name	String	Specifies the 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 Services Interconnected with Cloud Eye . Regex Pattern: <code>^([a-z] [A-Z]){1}([a-z] [A-Z] [0-9] _){1,32}\$</code>

Parameter	Type	Description
value	String	Specifies the 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] _ - \.)*)\ *){1,256}\$

Status code: 400

Table 6-214 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-215 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256

Parameter	Type	Description
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-216 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-217 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-218 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

Querying resources of a specified dimension and a specified service 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	Failed to verify parameters.
401	Not authenticated.

Status Code	Description
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.

URI

POST /v2/{project_id}/one-click-alarms

Table 6-219 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>

Request Parameters

Table 6-220 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Table 6-221 Request body parameters

Parameter	Mandatory	Type	Description
one_click_alarm_id	Yes	String	Specifies the one-click monitoring ID for a service.
dimension_names	Yes	DimensionNames object	Specifies 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	Specifies whether to enable the alarm notification.
alarm_notifications	No	Array of SMNAction objects	Specifies the action to be triggered by an alarm.
ok_notifications	No	Array of SMNAction objects	Specifies the action to be triggered after an alarm is cleared.
notification_begin_time	No	String	Specifies the time when the alarm notification was enabled.
notification_end_time	No	String	Specifies the time when the alarm notification was disabled.

Table 6-222 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. You must specify either metric or event .
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. You must specify either metric or event .

Table 6-223 SMNAction

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the notification type. The value can be notification , autoscaling , groupwatch , ecsRecovery , contact , contactGroup , or iecAction . Enumeration values: <ul style="list-style-type: none"> • notification • autoscaling • groupwatch • ecsRecovery • contact • contactGroup • iecAction Regex Pattern: ^(notification autoscaling groupwatch ecsRecovery contact contactGroup iecAction)\$

Parameter	Mandatory	Type	Description
notification_list	Yes	Array of strings	Specifies the 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 alarm_actions and ok_actions coexist, their notification_list values must be the same. Array Length: 0 - 20

Response Parameters

Status code: 201

Table 6-224 Response body parameters

Parameter	Type	Description
one_click_alarm_id	String	Specifies the one-click monitoring ID for a service.

Status code: 400

Table 6-225 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256

Parameter	Type	Description
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-226 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-227 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256

Parameter	Type	Description
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-228 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

```
{
  "one_click_alarm_id" : "o1234567890123456789012",
  "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"
}
```

Example Responses

Status code: 201

Created

```
{
  "one_click_alarm_id" : "o1234567890123456789012"
}
```

Status Codes

Status Code	Description
201	Created
400	Failed to verify parameters.
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.

URI

GET /v2/{project_id}/one-click-alarms

Table 6-229 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>

Request Parameters

Table 6-230 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-231 Response body parameters

Parameter	Type	Description
one_click_alarms	Array of one_click_alarms objects	Specifies services and resources that support one-click monitoring. Array Length: 1 - 1000

Table 6-232 one_click_alarms

Parameter	Type	Description
one_click_alarm_id	String	Specifies the one-click monitoring ID for a service.
namespace	String	Specifies the metric namespace.
description	String	Provides supplementary information about one-click monitoring. The description can contain 0 to 256 characters and is left blank by default.
enabled	Boolean	Specifies whether to enable one-click monitoring.

Status code: 400

Table 6-233 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-234 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service codes when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-235 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-236 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

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	Failed to verify parameters.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.10.3 Querying Alarm Rules of One Service in One-Click Monitoring

Function

This API is used to query alarm rules of one service in one-click monitoring.

URI

GET /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarms

Table 6-237 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>

Parameter	Mandatory	Type	Description
one_click_alarm_id	Yes	String	Specifies the one-click monitoring ID for a service. Minimum: 1 Maximum: 64

Request Parameters

Table 6-238 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-239 Response body parameters

Parameter	Type	Description
alarms	Array of alarms objects	Specifies the alarm rule list. Array Length: 1 - 100

Table 6-240 alarms

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

Parameter	Type	Description
name	String	Specifies the name of an alarm rule. The name can contain 1 to 128 characters, including only letters, digits, underscores (_), and hyphens (-).
description	String	Provides supplementary information about an alarm rule. The description can contain 0 to 256 characters.
namespace	String	Specifies the metric namespace.
policies	Array of Policy objects	Specifies the alarm policy. Array Length: 1 - 100
resources	Array of ResourcesInListResp objects	Specifies the resource list. Associated resources can be obtained by calling the API for querying resources in an alarm rule. Array Length: 1 - 3000
type	String	Specifies the alarm rule type.
enabled	Boolean	Specifies whether to generate alarms when the alarm triggering conditions are met.
notification_enabled	Boolean	Specifies whether to enable the alarm notification.
alarm_notifications	Array of SMNAction objects	Specifies the action to be triggered by an alarm.
ok_notifications	Array of SMNAction objects	Specifies the action to be triggered after an alarm is cleared.
notification_begin_time	String	Specifies the time when the alarm notification was enabled.
notification_end_time	String	Specifies the time when the alarm notification was disabled.

Table 6-241 Policy

Parameter	Type	Description
alarm_policy_id	String	Specifies the alarm policy ID.
metric_name	String	Specifies the metric name.

Parameter	Type	Description
period	Integer	Specifies how often to generate an alarm, in seconds. 1 indicates that alarms are generated based on raw data. When alarm_type is EVENT.SYS or EVENT.CUSTOM , the value may be 0 . Enumeration values: <ul style="list-style-type: none"> • 0 • 1 • 300 • 1200 • 3600 • 14400 • 86400
filter	String	Specifies the rollup method.
comparison_operator	String	Specifies the operator of an alarm threshold.
value	Number	Specifies the threshold.
unit	String	Specifies the metric unit.
count	Integer	Specifies the number of times that the alarm triggering conditions are met.
suppress_duration	Integer	Specifies the suppression period, in seconds. 0 indicates that only one alarm is generated. Enumeration values: <ul style="list-style-type: none"> • 0 • 300 • 600 • 900 • 1800 • 3600 • 10800 • 21600 • 43200 • 86400
level	Integer	Specifies the alarm severity, which can be 1 (critical), ** 2** (major), 3 (minor), or 4 (informational).

Parameter	Type	Description
enabled	Boolean	Specifies whether to enable one-click monitoring.

Table 6-242 ResourcesInListResp

Parameter	Type	Description
resource_group_id	String	Specifies the resource group ID. This parameter is available when the monitoring scope is resource groups. Regex Pattern: ^rg([a-z] [A-Z] [0-9]){2}\$
resource_group_name	String	Specifies the resource group name. This parameter is available when the monitoring scope is resource groups. Minimum: 1 Maximum: 128
dimensions	Array of MetricDimension objects	Specifies the dimension. Array Length: 0 - 10000

Table 6-243 MetricDimension

Parameter	Type	Description
name	String	Specifies the name of a metric dimension. Minimum: 1 Maximum: 32 Regex Pattern: ^([a-z] [A-Z]){1}([a-z] [A-Z] [0-9] _){1,32}\$
value	String	Specifies the value of a metric dimension. Minimum: 0 Maximum: 256 Regex Pattern: ^((([a-z] [A-Z] [0-9]){1}([a-z] [A-Z] [0-9] _)*))){0,256}\$

Table 6-244 SMNAction

Parameter	Type	Description
type	String	<p>Specifies the notification type. The value can be notification, autoscaling, groupwatch, ecsRecovery, contact, contactGroup, or iecAction.</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • notification • autoscaling • groupwatch • ecsRecovery • contact • contactGroup • iecAction <p>Regex Pattern: ^(notification autoscaling groupwatch ecsRecovery contact contactGroup iecAction)\$</p>
notification_list	Array of strings	<p>Specifies the 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 alarm_actions and ok_actions coexist, their notification_list values must be the same.</p> <p>Array Length: 0 - 20</p>

Status code: 400

Table 6-245 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-246 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-247 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-248 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

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": "alxxxxdsw12321321",
      "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"
  } ]
}
```

Status Codes

Status Code	Description
200	OK
400	Failed to verify parameters.
401	Not authenticated.
403	Authentication failed.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.10.4 Batch Enabling or Disabling Alarm Rules of One Service in One-Click Monitoring

Function

This API is used to batch enable or disable alarm rules for one service in one-click monitoring.

URI

PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarm-rules/action

Table 6-249 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>
one_click_alarm_id	Yes	String	Specifies the one-click monitoring ID for a service. Minimum: 1 Maximum: 64

Request Parameters

Table 6-250 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Table 6-251 Request body parameters

Parameter	Mandatory	Type	Description
alarm_ids	Yes	Array of strings	Specifies IDs of alarm rules to be enabled or disabled in batches. Array Length: 1 - 100
alarm_enabled	Yes	Boolean	Specifies whether to generate alarms when the alarm triggering conditions are met.

Response Parameters

Status code: 200

Table 6-252 Response body parameters

Parameter	Type	Description
alarm_ids	Array of strings	Specifies IDs of alarm rules that were enabled or disabled. Array Length: 1 - 100

Status code: 400

Table 6-253 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-254 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-255 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-256 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-257 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

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	Failed to verify parameters.
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 motoring.

URI

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

Table 6-258 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>

Request Parameters

Table 6-259 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Table 6-260 Request body parameters

Parameter	Mandatory	Type	Description
one_click_alarm_ids	Yes	Array of strings	Specifies IDs of services that need to disable one-click monitoring. Array Length: 1 - 100

Response Parameters

Status code: 200

Table 6-261 Response body parameters

Parameter	Type	Description
one_click_alarm_ids	Array of strings	Specifies IDs of services for which one-click monitoring was disabled. Array Length: 1 - 100

Status code: 400

Table 6-262 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-263 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-264 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-265 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

```
{
  "one_click_alarm_ids" : [ "o1619578505263QkW3b66yo" ]
}
```

Example Responses

Status code: 200

Specifies IDs of services for which one-click monitoring was disabled.

```
{
  "one_click_alarm_ids" : [ "o1619578505263QkW3b66yo" ]
}
```

Status Codes

Status Code	Description
200	Specifies IDs of services for which one-click monitoring was disabled.
400	Failed to verify parameters.
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 That Has 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.

URI

PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/notifications

Table 6-266 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>
one_click_alarm_id	Yes	String	Specifies the one-click monitoring ID for a service. Minimum: 1 Maximum: 64

Request Parameters

Table 6-267 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Table 6-268 Request body parameters

Parameter	Mandatory	Type	Description
notification_enabled	Yes	Boolean	Specifies whether to enable the alarm notification.
alarm_notifications	No	Array of SMNAction objects	Specifies the action to be triggered by an alarm.
ok_notifications	No	Array of SMNAction objects	Specifies the action to be triggered after an alarm is cleared.
notification_begin_time	No	String	Specifies the time when the alarm notification was enabled.
notification_end_time	No	String	Specifies the time when the alarm notification was disabled.

Table 6-269 SMNAction

Parameter	Mandatory	Type	Description
type	Yes	String	<p>Specifies the notification type. The value can be notification, autoscaling, groupwatch, ecsRecovery, contact, contactGroup, or iecAction.</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • notification • autoscaling • groupwatch • ecsRecovery • contact • contactGroup • iecAction <p>Regex Pattern: ^(notification autoscaling groupwatch ecsRecovery contact contactGroup iecAction)\$</p>
notification_list	Yes	Array of strings	<p>Specifies the 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 alarm_actions and ok_actions coexist, their notification_list values must be the same.</p> <p>Array Length: 0 - 20</p>

Response Parameters

Status code: 400

Table 6-270 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-271 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-272 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-273 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-274 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

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"
}
```

Example Responses

None

Status Codes

Status Code	Description
204	No Content
400	Failed to verify parameters.
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 Policies in Alarm Rules for One Service That Has One-Click Monitoring Enabled

Function

This API is used to batch enable or disable alarm policies in alarm rules for one service that has one-click monitoring enabled.

URI

PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarms/{alarm_id}/policies/action

Table 6-275 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>
one_click_alarm_id	Yes	String	Specifies the one-click monitoring ID for a service. Minimum: 1 Maximum: 64
alarm_id	Yes	String	Specifies the alarm rule ID. Minimum: 24 Maximum: 24

Request Parameters

Table 6-276 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Table 6-277 Request body parameters

Parameter	Mandatory	Type	Description
alarm_policy_ids	Yes	Array of strings	Specifies IDs of alarm policies to be enabled or disabled in batches in an alarm rule. Array Length: 1 - 100
enabled	Yes	Boolean	Specifies whether to enable one-click monitoring.

Response Parameters

Status code: 200

Table 6-278 Response body parameters

Parameter	Type	Description
alarm_policy_ids	Array of strings	Specifies IDs of alarm policies that were enabled or disabled in batches in an alarm rule. Array Length: 1 - 100

Status code: 400

Table 6-279 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-280 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 403

Table 6-281 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-282 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-283 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

```
{
  "alarm_policy_ids" : [ "alxdxxdsw12321321" ],
  "enabled" : true
}
```

Example Responses

Status code: 200

Alarm policies enabled or disabled.

```
{
  "alarm_policy_ids" : [ "alxdxxdsw12321321" ]
}
```

Status Codes

Status Code	Description
200	Alarm policies enabled or disabled.
400	Failed to verify parameters.
401	Not authenticated.
403	Authentication failed.
404	Resource not found.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.11 Alarm Notification Masking

6.11.1 Creating Alarm Notification Masking Rules in Batches

Function

This API is used to creating alarm notification masking rules in batches.

URI

PUT /v2/{project_id}/notification-masks

Table 6-284 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>

Request Parameters

Table 6-285 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Table 6-286 Request body parameters

Parameter	Mandatory	Type	Description
mask_name	No	String	Specifies the masking rule name. The value can contain up to 64 characters, including only letters, digits, hyphens (-), and underscores (_).
relation_type	Yes	String	Specifies the type of a resource that is associated with an alarm notification masking rule. ALARM_RULE : alarm rules RESOURCE : resources RESOURCE_POLICY_NOTIFICATION : alarm policies for the resource RESOURCE_POLICY_ALARM : alarm policies for the resource (The alarm policies are not used for alarm calculation.) Enumeration values: <ul style="list-style-type: none"> • ALARM_RULE • RESOURCE • RESOURCE_POLICY_NOTIFICATION • RESOURCE_POLICY_ALARM
relation_ids	Yes	Array of strings	Specifies the 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. Array Length: 1 - 100

Parameter	Mandatory	Type	Description
resources	No	Array of Resource objects	Specifies the resource for which alarm notifications will be masked when you set relation_type is to RESOURCE , RESOURCE_POLICY_NOTIFICATION , or RESOURCE_POLICY_ALARM . Array Length: 1 - 100
mask_type	Yes	String	Specifies the alarm notification 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: <ul style="list-style-type: none"> • START_END_TIME • FOREVER_TIME • CYCLE_TIME
start_date	No	String	Specifies the masking start date, in yyyy-MM-dd format.
start_time	No	String	Specifies the masking start time, in HH:mm:ss format.
end_date	No	String	Specifies the masking end date, in yyyy-MM-dd format.
end_time	No	String	Specifies the masking end time, in HH:mm:ss format.

Table 6-287 Resource

Parameter	Mandatory	Type	Description
namespace	Yes	String	Specifies the resource namespace in service.item format. The values of service and item must be character strings, start with a letter, and can contain digits, letters, and underscores (_). A namespace can contain 3 to 32 characters.

Parameter	Mandatory	Type	Description
dimensions	Yes	Array of Dimension objects	Specifies the resource dimension information. Array Length: 1 - 4

Table 6-288 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the 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 Services Interconnected with Cloud Eye . Regex Pattern: ^([a-z] [A-Z]){1}([a-z] [A-Z] [0-9] _ -){1,32}\$
value	Yes	String	Specifies the 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] _ \.)*)\)*){1,256}\$

Response Parameters

Status code: 201

Table 6-289 Response body parameters

Parameter	Type	Description
relation_ids	Array of strings	Specifies IDs of resources that were successfully associated with a masking rule. Array Length: 0 - 100
notification_mask_id	String	Specifies the masking rule ID.

Status code: 400

Table 6-290 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-291 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

```
{
  "mask_name": "mn_test",
  "relation_type": "ALARM_RULE",
  "relation_ids": [ "al123232232341232132" ],
  "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

Masking rules created.

```

{
  "relation_ids" : [ "al123232232341232132" ],
  "notification_mask_id" : "nm123232232341232132"
}

```

Status Codes

Status Code	Description
201	Masking rules created.
400	Failed to verify parameters.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.11.2 Modifying the Masking Time of Alarm Notification Masking Rules in Batches

Function

This API is used to modify the masking time of alarm notification masking rules in batches.

URI

POST /v2/{project_id}/notification-masks/batch-update

Table 6-292 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>

Request Parameters

Table 6-293 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Table 6-294 Request body parameters

Parameter	Mandatory	Type	Description
notification_mask_ids	Yes	Array of strings	Specifies the associated ID. Array Length: 1 - 100

Parameter	Mandatory	Type	Description
mask_type	Yes	String	Specifies the alarm notification 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: <ul style="list-style-type: none"> • START_END_TIME • FOREVER_TIME • CYCLE_TIME
start_date	No	String	Specifies the masking start date, in yyyy-MM-dd format.
start_time	No	String	Specifies the masking start time, in HH:mm:ss format.
end_date	No	String	Specifies the masking end date, in yyyy-MM-dd format.
end_time	No	String	Specifies the masking end time, in HH:mm:ss format.

Response Parameters

Status code: 400

Table 6-295 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-296 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

```
{
  "notification_mask_ids" : [ "nm123232232341232132" ],
  "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.
400	Failed to verify parameters.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.11.3 Modifying an Alarm Notification Masking Rule

Function

This API is used to modify an alarm notification masking rule.

URI

PUT /v2/{project_id}/notification-masks/{notification_mask_id}

Table 6-297 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>
notification_mask_id	Yes	String	Specifies the masking rule ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^([a-z] [A-Z] [0-9]){1,64}\$</code>

Request Parameters

Table 6-298 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Table 6-299 Request body parameters

Parameter	Mandatory	Type	Description
mask_name	Yes	String	Specifies the masking rule name. The value can contain up to 64 characters, including only letters, digits, hyphens (-), and underscores (_).
relation_ids	No	Array of strings	Specifies the 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. Array Length: 1 - 100
relation_type	No	String	Specifies the type of a resource that is associated with an alarm notification masking rule. ALARM_RULE : alarm rules RESOURCE : resources RESOURCE_POLICY_NOTIFICATION : alarm policies for the resource RESOURCE_POLICY_ALARM : alarm policies for the resource (The alarm policies are not used for alarm calculation.) Enumeration values: <ul style="list-style-type: none"> • ALARM_RULE • RESOURCE • RESOURCE_POLICY_NOTIFICATION • RESOURCE_POLICY_ALARM
resources	Yes	Array of Resource objects	Specifies the associated resource. Array Length: 1 - 100

Parameter	Mandatory	Type	Description
mask_type	Yes	String	Specifies the alarm notification 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: <ul style="list-style-type: none"> • START_END_TIME • FOREVER_TIME • CYCLE_TIME
start_date	No	String	Specifies the masking start date, in yyyy-MM-dd format.
start_time	No	String	Specifies the masking start time, in HH:mm:ss format.
end_date	No	String	Specifies the masking end date, in yyyy-MM-dd format.
end_time	No	String	Specifies the masking end time, in HH:mm:ss format.

Table 6-300 Resource

Parameter	Mandatory	Type	Description
namespace	Yes	String	Specifies the resource namespace in service.item format. The values of service and item must be character strings, start with a letter, and can contain digits, letters, and underscores (_). A namespace can contain 3 to 32 characters.
dimensions	Yes	Array of Dimension objects	Specifies the resource dimension information. Array Length: 1 - 4

Table 6-301 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the 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 Services Interconnected with Cloud Eye . Regex Pattern: ^([a-z] [A-Z]){1}([a-z] [A-Z] [0-9] _ -){1,32}\$
value	Yes	String	Specifies the 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] _ \.)*)\ *){1,256})\$

Response Parameters

Status code: 400

Table 6-302 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-303 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

```
{
  "mask_name": "mn_test",
  "relation_ids": [ "al123232232341232132" ],
  "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	Failed to verify parameters.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.11.4 Deleting Alarm Notification Masking Rules in Batches

Function

This API is used to deleting alarm notification masking rules in batches.

URI

POST /v2/{project_id}/notification-masks/batch-delete

Table 6-304 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>

Request Parameters

Table 6-305 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Table 6-306 Request body parameters

Parameter	Mandatory	Type	Description
notification_mask_ids	Yes	Array of strings	Specifies the masking rule ID. Array Length: 1 - 100

Response Parameters

Status code: 200

Table 6-307 Response body parameters

Parameter	Type	Description
notification_mask_ids	Array of strings	Specifies the ID of a masking rule that was successfully deleted. Array Length: 1 - 100

Status code: 400

Table 6-308 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-309 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-310 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Example Requests

```
{
  "notification_mask_ids" : [ "nm123232232341232132" ]
}
```

Example Responses

Status code: 200

Notification masking rules deleted.

```
{
  "notification_mask_ids" : [ "nm123232232341232132" ]
}
```

Status Codes

Status Code	Description
200	Notification masking rules deleted.
400	Failed to verify parameters.
404	Resource not found.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.11.5 Querying Alarm Notification 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.

URI

POST /v2/{project_id}/notification-masks/batch-query

Table 6-311 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>

Table 6-312 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Specifies the pagination offset. Minimum: 0 Maximum: 10000 Default: 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	Specifies the number of records that will be displayed on each page. Minimum: 1 Maximum: 100 Default: 100 Regex Pattern: ^([1-9] [1-9][0-9] 100)\$

Request Parameters

Table 6-313 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Table 6-314 Request body parameters

Parameter	Mandatory	Type	Description
relation_type	Yes	String	<p>Specifies the type of a resource that is associated with an alarm notification masking rule. ALARM_RULE: alarm rules RESOURCE: resources RESOURCE_POLICY_NOTIFICATION: alarm policies for the resource RESOURCE_POLICY_ALARM: alarm policies for the resource (The alarm policies are not used for alarm calculation.) DEFAULT: By default, RESOURCE and RESOURCE_POLICY_NOTIFICATION (used for querying alarm notification masking rules) are included.</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • ALARM_RULE • RESOURCE • RESOURCE_POLICY_NOTIFICATION • RESOURCE_POLICY_ALARM • DEFAULT
relation_ids	Yes	Array of strings	<p>Specifies the ID of the alarm rule that is associated with the alarm notification masking rule.</p> <p>Array Length: 1 - 100</p>
mask_id	No	String	<p>(Optional) Specifies the masking rule ID.</p> <p>Minimum: 1</p> <p>Maximum: 64</p> <p>Regex Pattern: ^nm([0-9A-Za-z]){0,62}\$</p>

Parameter	Mandatory	Type	Description
mask_name	No	String	Specifies the masking rule name. The value can contain up to 64 characters, including only letters, digits, hyphens (-), and underscores (_). Minimum: 1 Maximum: 64 Regex Pattern: ^([\u4E00-\u9FFF] [a-z] [A-Z] [0-9] _)+\$
mask_status	No	String	(Optional) Specifies whether a masking rule is in effect. MASK_EFFECTIVE: The masking rule is in effect. MASK_INEFFECTIVE: The masking rule is not in effect. Minimum: 1 Maximum: 32 Enumeration values: <ul style="list-style-type: none"> • MASK_EFFECTIVE • MASK_INEFFECTIVE
resource_id	No	String	(Optional) Specifies the resource dimension value. You can specify one or more resource IDs from one dimension. Minimum: 1 Maximum: 700
namespace	No	String	Specifies the resource namespace in service.item format. The values of service and item must be character strings, start with a letter, and can contain digits, letters, and underscores (_). A namespace can contain 3 to 32 characters.
dimensions	No	Array of Dimension objects	Specifies the resource dimension information. Array Length: 1 - 4

Table 6-315 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the 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 Services Interconnected with Cloud Eye . Regex Pattern: ^([a-z] [A-Z]){1}([a-z] [A-Z] [0-9] _ -){1,32}\$
value	Yes	String	Specifies the 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] _ \.)*)\)*{1,256})\$

Response Parameters

Status code: 200

Table 6-316 Response body parameters

Parameter	Type	Description
notification_masks	Array of notification_masks objects	Specifies the list of alarm notification masking rules. Array Length: 1 - 100
count	Integer	Specifies the total number of alarm notification masking rules. Minimum: 0 Maximum: 99999

Table 6-317 notification_masks

Parameter	Type	Description
notification_mask_id	String	Specifies the masking rule ID.
mask_name	String	Specifies the masking rule name. The value can contain up to 64 characters, including only letters, digits, hyphens (-), and underscores (_).
relation_type	String	Specifies the type of a resource that is associated with an alarm notification masking rule. ALARM_RULE : alarm rules RESOURCE : resources RESOURCE_POLICY_NOTIFICATION : alarm policies for the resource RESOURCE_POLICY_ALARM : alarm policies for the resource (The alarm policies are not used for alarm calculation.) Enumeration values: <ul style="list-style-type: none"> • ALARM_RULE • RESOURCE • RESOURCE_POLICY_NOTIFICATION • RESOURCE_POLICY_ALARM
relation_id	String	Specifies the associated ID.
resources	Array of ResourceCategory objects	Specifies the 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. Array Length: 1 - 100
mask_status	String	Specifies whether alarm notifications are masked. UN_MASKED : Alarm notifications are not masked. MASK_EFFECTIVE : Masking rules are in effect. MASK_INEFFECTIVE : Masking rules are not in effect. Enumeration values: <ul style="list-style-type: none"> • UN_MASKED • MASK_EFFECTIVE • MASK_INEFFECTIVE

Parameter	Type	Description
mask_type	String	Specifies the alarm notification 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: <ul style="list-style-type: none"> • START_END_TIME • FOREVER_TIME • CYCLE_TIME
start_date	String	Specifies the masking start date, in yyyy-MM-dd format.
start_time	String	Specifies the masking start time, in HH:mm:ss format.
end_date	String	Specifies the masking end date, in yyyy-MM-dd format.
end_time	String	Specifies the masking end time, in HH:mm:ss format.
policies	Array of PoliciesInListResponse objects	Specifies the alarm policy list. Array Length: 0 - 50

Table 6-318 ResourceCategory

Parameter	Type	Description
namespace	String	Specifies the resource namespace in service.item format. The values of service and item must be character strings, start with a letter, and can contain digits, letters, and underscores (_). A namespace can contain 3 to 32 characters.
dimension_names	Array of strings	Specifies the resource dimension information. Multiple dimensions are sorted in alphabetical order and separated with commas (,). Minimum: 1 Maximum: 131 Array Length: 1 - 100

Table 6-319 PoliciesInListResp

Parameter	Type	Description
alarm_policy_id	String	Specifies the alarm policy ID.
metric_name	String	Specifies the 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	Specifies the extended metric information.
period	Integer	Specifies the period for determining whether to generate an alarm, in seconds. The value can be 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 or EVENT.CUSTOM . Enumeration values: <ul style="list-style-type: none"> • 1 • 300 • 1200 • 3600 • 14400 • 86400
filter	String	Specifies the data rollup method. The value can be max, min, average, sum, or variance . Enumeration values: <ul style="list-style-type: none"> • max • min • average • sum • variance

Parameter	Type	Description
comparison_operator	String	<p>Specifies the operator, which can be >, =, <, >=, <=, !=, cycle_decrease, cycle_increase, or cycle_wave.</p> <p>cycle_decrease indicates a decrease compared with the last period.</p> <p>cycle_increase indicates an increase compared with the last period.</p> <p>cycle_wave indicates an increase or decrease compared with the last period.</p> <p>Enumeration values:</p> <ul style="list-style-type: none"> • > • = • < • >= • <= • != • cycle_decrease • cycle_increase • cycle_wave
value	Number	<p>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. The value ranges from 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. 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. (tag: dt,g42,dt_test,hk_g42,hk_sbc,hws,hws_hk,ocb,sbc,tm)</p>
unit	String	Specifies the data unit.
count	Integer	Specifies the number of consecutive times that alarm conditions are met. Supported range: 1 to 5

Parameter	Type	Description
type	String	Specifies the alarm policy type. (This parameter is not used currently.) Minimum: 0 Maximum: 32
suppress_duration	Integer	Specifies the 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: <ul style="list-style-type: none"> • 0 • 300 • 600 • 900 • 1800 • 3600 • 10800 • 21600 • 43200 • 86400
alarm_level	Integer	Specifies the alarm severity. The value 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 6-320 MetricExtraInfo

Parameter	Type	Description
origin_metric_name	String	Specifies the original metric name. Minimum: 1 Maximum: 4096 Regex Pattern: ^([a-z] [A-Z] [0-9] _ ~ \./ :)*\$
metric_prefix	String	Specifies the metric name prefix. Minimum: 1 Maximum: 4096 Regex Pattern: ^([a-z] [A-Z] [0-9] _ ~ \./ :)*\$
custom_proc_name	String	Specifies the name of a user process. Minimum: 1 Maximum: 250
metric_type	String	Specifies the metric type. Minimum: 1 Maximum: 32 Regex Pattern: ^([a-z] [A-Z] [0-9] _ ~ \./ :)*\$

Status code: 400

Table 6-321 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-322 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

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",
    "resources": [ {
      "namespace": "SYS.ECS",
      "dimension_names": [ "disk_utils,instance_id" ]
    } ],
    "mask_status": "UN_MASKED",
    "mask_type": "START_END_TIME",
    "start_date": "yyy-MM-dd",
    "start_time": "HH:mm:ss",
    "end_date": "yyy-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" : "SIAsh_",
    "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	Failed to verify parameters.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.11.6 Querying Resources for Which Alarm Notifications Have Been Masked

Function

This API is used to query resources for which alarm notifications have been masked.

URI

GET /v2/{project_id}/notification-masks/{notification_mask_id}/resources

Table 6-323 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>
notification_mask_id	Yes	String	Specifies the masking rule ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^([a-z] [A-Z] [0-9]){1,64}\$</code>

Table 6-324 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Specifies the pagination offset. Minimum: 0 Maximum: 10000 Default: 0 Regex Pattern: <code>^([0] [1-9] [1-9][0-9] [1-9][0-9][0-9] [1-9][0-9][0-9][0-9] 10000)\$</code>
limit	No	Integer	Specifies the number of records that will be displayed on each page. Minimum: 1 Maximum: 100 Default: 100 Regex Pattern: <code>^([1-9] [1-9][0-9] 100)\$</code>

Request Parameters

Table 6-325 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-326 Response body parameters

Parameter	Type	Description
resources	Array of Resource objects	Specifies the list of resources whose alarm notifications are masked. Array Length: 1 - 100
count	Integer	Specifies the total number of resources. Minimum: 0 Maximum: 100

Table 6-327 Resource

Parameter	Type	Description
namespace	String	Specifies the resource namespace in service.item format. The values of service and item must be character strings, start with a letter, and can contain digits, letters, and underscores (_). A namespace can contain 3 to 32 characters.

Parameter	Type	Description
dimensions	Array of Dimension objects	Specifies the resource dimension information. Array Length: 1 - 4

Table 6-328 Dimension

Parameter	Type	Description
name	String	Specifies the 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 Services Interconnected with Cloud Eye . Regex Pattern: ^([a-z] [A-Z]){1}([a-z] [A-Z] [0-9] _ -){1,32}\$
value	String	Specifies the 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] _ - \.)*)\)*\)*{1,256}\$

Status code: 400

Table 6-329 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-330 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Specifies the request error message. Minimum: 0 Maximum: 256
request_id	String	Specifies the request ID. Minimum: 0 Maximum: 256

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	Failed to verify parameters.
500	Internal system error.

Error Codes

See [Error Codes](#).

6.12 Dashboards

6.12.1 This API is used to create or copy a dashboard.

Function

This API is used to create or copy a dashboard.

Constraints

This API is not supported in the following five sites: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, and ME-Riyadh.

URI

POST /v2/{project_id}/dashboards

Table 6-331 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID. Minimum: 1 Maximum: 64

Request Parameters

Table 6-332 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	MIME type of the request body. Default value application/json is recommended. Default: application/json;charset=UTF-8 Minimum: 1 Maximum: 64

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It is a response to the API used to obtain 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 value. Minimum: 1 Maximum: 16000

Table 6-333 Request body parameters

Parameter	Mandatory	Type	Description
dashboard_name	Yes	String	Custom name of the dashboard. Minimum: 1 Maximum: 128 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_number	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. Minimum: 0 Maximum: 3 Default: 3

Response Parameters

Status code: 201

Table 6-334 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 6-335 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-336 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-337 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Example Requests

```
{
  "dashboard_name" : "dashboard_name",
  "enterprise_id" : "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "dashboard_id" : "dbxxxxxxxxxxxxxxxxxxxx",
  "row_widget_num" : 3
}
```

Example Responses

Status code: 201

OK

```
{
  "dashboard_id" : "dbxxxxxxxx"
}
```

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 five regions: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, and ME-Riyadh.

URI

GET /v2/{project_id}/dashboards

Table 6-338 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID. Minimum: 1 Maximum: 64

Table 6-339 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.

Parameter	Mandatory	Type	Description
dashboard_name	No	String	Dashboard name. Minimum: 1 Maximum: 128 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}

Request Parameters

Table 6-340 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It is a response to the API used to obtain 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 value. Minimum: 1 Maximum: 16000

Response Parameters

Status code: 200

Table 6-341 Response body parameters

Parameter	Type	Description
dashboards	Array of DashBoardInfo objects	Dashboard list. Array Length: 0 - 10

Table 6-342 DashBoardInfo

Parameter	Type	Description
dashboard_id	String	Dashboard ID. Regex Pattern: ^db([a-z] [A-Z] [0-9]){22}
dashboard_name	String	Custom name of the dashboard. Minimum: 1 Maximum: 128 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. Minimum: 1 Maximum: 128 Regex Pattern: ^([\u4E00-\u9FFF] [a-z] [A-Z] [0-9] _ -)+\$
create_time	Long	Dashboard creation time. Minimum: 11111111111111 Maximum: 99999999999999
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. Minimum: 0 Maximum: 3 Default: 3
is_favorite	Boolean	Whether a dashboard is added to favorites. The value can be true or false .

Status code: 400

Table 6-343 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-344 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-345 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256

Parameter	Type	Description
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "dashboards": [ {
    "dashboard_id": "dbxxxxxxxxxxxxxxxxxxxx",
    "dashboard_name": "dashboard_name",
    "enterprise_id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "creator_name": "creator_name",
    "create_time": 11111111111111,
    "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 five sites: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, and ME-Riyadh.

URI

PUT /v2/{project_id}/dashboards/{dashboard_id}

Table 6-346 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID. Minimum: 1 Maximum: 64
dashboard_id	Yes	String	Dashboard ID, which starts with db and follows 22 letters and digits. Example: db16564943172807wjOmOlyn Array Length: 24 - 24 Regex Pattern: <code>^db([a-z] [A-Z] [0-9]){22}\$</code>

Request Parameters

Table 6-347 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	MIME type of the request body. Default value application/json is recommended. Default: application/json;charset=UTF-8 Minimum: 1 Maximum: 64

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token. It is a response to the API used to obtain 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 value. Minimum: 1 Maximum: 16000

Table 6-348 Request body parameters

Parameter	Mandatory	Type	Description
dashboard_name	No	String	Custom name of the dashboard. Minimum: 1 Maximum: 128 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 .
row_widget_number	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. Minimum: 0 Maximum: 3 Default: 3

Response Parameters

Status code: **400**

Table 6-349 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-350 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-351 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256

Parameter	Type	Description
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

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 This API is used to delete dashboards in batches.

Function

This API is used to delete dashboards in batches.

Constraints

This API is not supported in the following five sites: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, and ME-Riyadh.

URI

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

Table 6-352 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID. Minimum: 1 Maximum: 64

Request Parameters

Table 6-353 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	MIME type of the request body. Default value application/json is recommended. Default: application/json;charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	User token. It is a response to the API used to obtain 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 value. Minimum: 1 Maximum: 16000

Table 6-354 Request body parameters

Parameter	Mandatory	Type	Description
dashboard_ids	No	Array of strings	Dashboard ID list. Array Length: 1 - 30

Response Parameters

Status code: 200

Table 6-355 Response body parameters

Parameter	Type	Description
dashboards	Array of BatchDeleteDashboardRespInfo objects	Response body for deleting dashboards in batches. Array Length: 1 - 100

Table 6-356 BatchDeleteDashboardRespInfo

Parameter	Type	Description
dashboard_id	String	Dashboard ID. Regex Pattern: ^db([a-z] [A-Z] [0-9]){2}
ret_status	String	Operation result. The value can be successful or error . Enumeration values: <ul style="list-style-type: none"> • successful • error
error_msg	String	Error message. Minimum: 0 Maximum: 128

Status code: 400

Table 6-357 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256

Parameter	Type	Description
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-358 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-359 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Example Requests

```
{  
  "dashboard_ids" : [ "dbxxxxxxxxxxxxxxxxxxxx", "dbXXXXXXXXXXXXXXXXXXXX" ]  
}
```

Example Responses

Status code: 200

OK

```
{  
  "dashboards" : [ {  
    "dashboard_id" : "dbxxxxxxxxxxxxxxxxxxxx",  
    "ret_status" : "successful"  
  }, {  
    "dashboard_id" : "dbXXXXXXXXXXXXXXXXXXXX",  
    "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 This API is used to create, copy, or batch create 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 five sites: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, and ME-Riyadh.

URI

POST /v2/{project_id}/dashboards/{dashboard_id}/widgets

Table 6-360 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID. Minimum: 1 Maximum: 64
dashboard_id	Yes	String	Dashboard ID, which starts with db and follows 22 letters and digits. Example: db16564943172807wjOmOlyn Array Length: 24 - 24 Regex Pattern: <code>^db([a-z] [A-Z] [0-9]){22}\$</code>

Request Parameters

Table 6-361 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	MIME type of the request body. Default value application/json is recommended. Default: application/json;charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	User token. It is a response to the API used to obtain 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 value. Minimum: 1 Maximum: 16000

Table 6-362 Request body parameters

Parameter	Mandatory	Type	Description
[items]	No	Array of BaseWidgetInfo objects	Graph information.

Table 6-363 BaseWidgetInfo

Parameter	Mandatory	Type	Description
metrics	Yes	Array of WidgetMetric objects	Metric list. Array Length: 1 - 200
title	Yes	String	Graph name. Minimum: 1 Maximum: 128 Regex Pattern: ^([\u4E00-\u9FFF] [a-z] [A-Z] [0-9] _ - : ; \\(\\) \\. ~ ())+\$
threshold	No	Double	Threshold of metrics on the graph. Minimum: 0 Maximum: 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	Monitoring view chart type. The options are bar , line , bar_chart , table , circular_bar , and area_chart . Enumeration values: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • single • multiple
properties	No	properties object	Additional information.
location	Yes	location object	Graph coordinates.
unit	No	String	Unit.

Table 6-364 WidgetMetric

Parameter	Mandatory	Type	Description
namespace	Yes	String	Cloud service dimension. Minimum: 3 Maximum: 32 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. Minimum: 1 Maximum: 96 Regex Pattern: ^([A-Za-z]){1}([0-9A-Za-z] _ -)*\$
alias	No	Array of strings	Alias list of metrics on the graph. Minimum: 1 Maximum: 128 Array Length: 0 - 200
extra_info	No	ExtraInfo object	Metric information.

Table 6-365 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 . Minimum: 1 Maximum: 131 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}\$
filter_type	Yes	String	Resource type. The value can be all_instances (all resources) or specific_instances (specified resources). Enumeration values: <ul style="list-style-type: none"> • all_instances • specific_instances
values	No	Array of strings	Dimension value list. Minimum: 1 Maximum: 1024 Array Length: 0 - 200

Table 6-366 ExtraInfo

Parameter	Mandatory	Type	Description
origin_metric_name	Yes	String	Metric name. Minimum: 1 Maximum: 4096 Regex Pattern: ^([a-z] [A-Z] [0-9] _ ~ \. / :)*\$
metric_prefix	No	String	Metric name prefix. Minimum: 1 Maximum: 4096 Regex Pattern: ^([a-z] [A-Z] [0-9] _ ~ \. / :)*\$

Parameter	Mandatory	Type	Description
metric_type	No	String	Metric type. Minimum: 1 Maximum: 32 Regex Pattern: ^([a-z] [A-Z] [0-9] _ ~ \. / :)*\$
custom_proc_name	No	String	Custom process name. Minimum: 1 Maximum: 250

Table 6-367 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: <ul style="list-style-type: none"> • 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. Minimum: 1 Maximum: 2147483647 Default: 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: <ul style="list-style-type: none"> • asc • desc

Table 6-368 location

Parameter	Mandatory	Type	Description
top	Yes	Integer	Grids between the graph and the top of the dashboard. Minimum: 0 Maximum: 2147483647
left	Yes	Integer	Grids between the graph and the left side of the dashboard. Minimum: 0 Maximum: 9
width	Yes	Integer	Graph width. Minimum: 3 Maximum: 12
height	Yes	Integer	Graph height. Minimum: 3 Maximum: 2147483647

Response Parameters

Status code: 200

Table 6-369 Response body parameters

Parameter	Type	Description
widget_ids	Array of strings	Response body for creating graphs in batches. Array Length: 1 - 50

Status code: 400

Table 6-370 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256

Parameter	Type	Description
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-371 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-372 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256

Parameter	Type	Description
request_id	String	Request ID. Minimum: 0 Maximum: 256

Example Requests

```
[ {
  "metrics" : [ {
    "namespace" : "SYS.ECS",
    "dimensions" : {
      "name" : "instance_id",
      "filter_type" : "specific_instances",
      "values" : [ "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" ]
    },
    "metric_name" : "cpu_util",
    "alias" : [ "cpuutilias" ],
    "extra_info" : {
      "origin_metric_name" : "cpu_util",
      "metric_prefix" : "cpu",
      "metric_type" : "type",
      "custom_proc_name" : "app.sh"
    }
  } ],
  "view" : "view",
  "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

Status Code	Description
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 five sites: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, and ME-Riyadh.

URI

GET /v2/{project_id}/dashboards/{dashboard_id}/widgets

Table 6-373 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID. Minimum: 1 Maximum: 64
dashboard_id	Yes	String	Dashboard ID, which starts with db and follows 22 letters and digits. Example: db16564943172807wjOmOlyn Array Length: 24 - 24 Regex Pattern: <code>^db([a-z] [A-Z] [0-9]){22}\$</code>

Table 6-374 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 6-375 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	MIME type of the request body. Default value application/json is recommended. Default: application/json;charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	User token. It is a response to the API used to obtain 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 value. Minimum: 1 Maximum: 16000

Response Parameters

Status code: 200

Table 6-376 Response body parameters

Parameter	Type	Description
widgets	Array of WidgetInfoWithId objects	Graph list. Array Length: 0 - 50

Table 6-377 WidgetInfoWithId

Parameter	Type	Description
widget_id	String	Graph ID. Regex Pattern: ^wg([a-z] [A-Z] [0-9]){2}\$
metrics	Array of WidgetMetric objects	Metric list. Array Length: 1 - 200
title	String	Graph name. Minimum: 1 Maximum: 128 Regex Pattern: ^([\u4E00-\u9FFF] [a-z] [A-Z] [0-9] _ - : ; \\(\\) \\. ~ ())+\$
threshold	Double	Threshold of metrics on the graph. Minimum: 0 Maximum: 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	Monitoring view chart type. The options are bar , line , bar_chart , table , circular_bar , and area_chart . Enumeration values: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • single • multiple
properties	properties object	Additional information.
location	location object	Graph coordinates.
unit	String	Unit.

Parameter	Type	Description
create_time	Long	Dashboard creation time. Minimum: 11111111111111 Maximum: 99999999999999

Table 6-378 WidgetMetric

Parameter	Type	Description
namespace	String	Cloud service dimension. Minimum: 3 Maximum: 32 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. Minimum: 1 Maximum: 96 Regex Pattern: ^([A-Za-z]){1}([0-9A-Za-z] _ -)*\$
alias	Array of strings	Alias list of metrics on the graph. Minimum: 1 Maximum: 128 Array Length: 0 - 200
extra_info	ExtraInfo object	Metric information.

Table 6-379 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 . Minimum: 1 Maximum: 131 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}\$
filter_type	String	Resource type. The value can be all_instances (all resources) or specific_instances (specified resources). Enumeration values: <ul style="list-style-type: none"> • all_instances • specific_instances
values	Array of strings	Dimension value list. Minimum: 1 Maximum: 1024 Array Length: 0 - 200

Table 6-380 ExtraInfo

Parameter	Type	Description
origin_metric_name	String	Metric name. Minimum: 1 Maximum: 4096 Regex Pattern: ^([a-z] [A-Z] [0-9] _ - ~\./ :)*\$
metric_prefix	String	Metric name prefix. Minimum: 1 Maximum: 4096 Regex Pattern: ^([a-z] [A-Z] [0-9] _ - ~\./ :)*\$

Parameter	Type	Description
metric_type	String	Metric type. Minimum: 1 Maximum: 32 Regex Pattern: ^([a-z] [A-Z] [0-9] _ - ~ \./ !)*\$
custom_proc_name	String	Custom process name. Minimum: 1 Maximum: 250

Table 6-381 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: <ul style="list-style-type: none"> • topN
topN	Integer	Top N values. In the line chart, this parameter indicates the number of time series data records that are randomly displayed. Minimum: 1 Maximum: 2147483647 Default: 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: <ul style="list-style-type: none"> • asc • desc

Table 6-382 location

Parameter	Type	Description
top	Integer	Grids between the graph and the top of the dashboard. Minimum: 0 Maximum: 2147483647
left	Integer	Grids between the graph and the left side of the dashboard. Minimum: 0 Maximum: 9
width	Integer	Graph width. Minimum: 3 Maximum: 12
height	Integer	Graph height. Minimum: 3 Maximum: 2147483647

Status code: 400

Table 6-383 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-384 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-385 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Example Requests

None

Example Responses

Status code: 200

OK

```
[ {
  "widget_id" : "wg1234567890123456789012",
  "metrics" : [ {
```



```

"namespace" : "SYS.ECS",
"dimensions" : {
  "name" : "instance_id",
  "filter_type" : "specific_instances",
  "values" : [ "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" ],
  "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" : "view",
"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" : 11111111111111
}]

```

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 five sites: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, and ME-Riyadh.

URI

GET /v2/{project_id}/widgets/{widget_id}

Table 6-386 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID. Minimum: 1 Maximum: 64
widget_id	Yes	String	Graph ID. Regex Pattern: ^wg([a-z] [A-Z] [0-9]){22}\$

Request Parameters

Table 6-387 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	MIME type of the request body. Default value application/json is recommended. Default: application/json;charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	User token. It is a response to the API used to obtain 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 value. Minimum: 1 Maximum: 16000

Response Parameters

Status code: 200

Table 6-388 Response body parameters

Parameter	Type	Description
widget_id	String	Graph ID. Regex Pattern: ^wg([a-z] [A-Z] [0-9]){2}\$
metrics	Array of WidgetMetric objects	Metric list. Array Length: 1 - 200
title	String	Graph name. Minimum: 1 Maximum: 128 Regex Pattern: ^([\u4E00-\u9FFF] [a-z] [A-Z] [0-9] _ - : ; \(\) \~ ())+\$
threshold	Double	Threshold of metrics on the graph. Minimum: 0 Maximum: 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	Monitoring view chart type. The options are bar , line , bar_chart , table , circular_bar , and area_chart . Enumeration values: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • single • multiple
properties	properties object	Additional information.
location	location object	Graph coordinates.

Parameter	Type	Description
unit	String	Unit.
create_time	Long	Dashboard creation time. Minimum: 111111111111 Maximum: 999999999999

Table 6-389 WidgetMetric

Parameter	Type	Description
namespace	String	Cloud service dimension. Minimum: 3 Maximum: 32 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. Minimum: 1 Maximum: 96 Regex Pattern: ^([A-Za-z]){1}([0-9A-Za-z] _)*\$
alias	Array of strings	Alias list of metrics on the graph. Minimum: 1 Maximum: 128 Array Length: 0 - 200
extra_info	ExtraInfo object	Metric information.

Table 6-390 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 . Minimum: 1 Maximum: 131 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}\$
filter_type	String	Resource type. The value can be all_instances (all resources) or specific_instances (specified resources). Enumeration values: <ul style="list-style-type: none"> • all_instances • specific_instances
values	Array of strings	Dimension value list. Minimum: 1 Maximum: 1024 Array Length: 0 - 200

Table 6-391 ExtraInfo

Parameter	Type	Description
origin_metric_name	String	Metric name. Minimum: 1 Maximum: 4096 Regex Pattern: ^([a-z] [A-Z] [0-9] _ - ~\./ :)*\$
metric_prefix	String	Metric name prefix. Minimum: 1 Maximum: 4096 Regex Pattern: ^([a-z] [A-Z] [0-9] _ - ~\./ :)*\$

Parameter	Type	Description
metric_type	String	Metric type. Minimum: 1 Maximum: 32 Regex Pattern: ^([a-z] [A-Z] [0-9] _ ~ \./ !)*\$
custom_proc_name	String	Custom process name. Minimum: 1 Maximum: 250

Table 6-392 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: <ul style="list-style-type: none"> • topN
topN	Integer	Top N values. In the line chart, this parameter indicates the number of time series data records that are randomly displayed. Minimum: 1 Maximum: 2147483647 Default: 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: <ul style="list-style-type: none"> • asc • desc

Table 6-393 location

Parameter	Type	Description
top	Integer	Grids between the graph and the top of the dashboard. Minimum: 0 Maximum: 2147483647
left	Integer	Grids between the graph and the left side of the dashboard. Minimum: 0 Maximum: 9
width	Integer	Graph width. Minimum: 3 Maximum: 12
height	Integer	Graph height. Minimum: 3 Maximum: 2147483647

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. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

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. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

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. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Example Requests

None

Example Responses

Status code: 200

OK

```
{
  "widget_id" : "wg1234567890123456789012",
  "metrics" : [ {
```



```

"namespace" : "SYS.ECS",
"dimensions" : {
  "name" : "instance_id",
  "filter_type" : "specific_instances",
  "values" : [ "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" ]
},
"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" : "view",
"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" : 111111111111
}

```

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 five sites: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, and ME-Riyadh.

URI

DELETE /v2/{project_id}/widgets/{widget_id}

Table 6-397 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID. Minimum: 1 Maximum: 64
widget_id	Yes	String	Graph ID. Regex Pattern: ^wg([a-z] [A-Z] [0-9]){22}\$

Request Parameters

Table 6-398 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	MIME type of the request body. Default value application/json is recommended. Default: application/json;charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	User token. It is a response to the API used to obtain 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 value. Minimum: 1 Maximum: 16000

Response Parameters

Status code: 400

Table 6-399 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-400 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-401 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Example Requests

None

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](#).

6.13.5 Updating Graphs in Batches

Function

This API is used to update graphs in batches.

Constraints

This API is not supported in the following five sites: CN East-Qingdao, LA-Mexico City1, TR-Istanbul, AP-Jakarta, and ME-Riyadh.

URI

POST /v2/{project_id}/widgets/batch-update

Table 6-402 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Tenant ID. Minimum: 1 Maximum: 64

Request Parameters

Table 6-403 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	MIME type of the request body. Default value application/json is recommended. Default: application/json;charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	User token. It is a response to the API used to obtain 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 value. Minimum: 1 Maximum: 16000

Table 6-404 Request body parameters

Parameter	Mandatory	Type	Description
[items]	Yes	Array of UpdateWidgetInfo objects	List of graphs to be modified.

Table 6-405 UpdateWidgetInfo

Parameter	Mandatory	Type	Description
widget_id	Yes	String	Graph ID. Regex Pattern: <code>^wg([a-z][A-Z][0-9]){22}\$</code>
metrics	No	Array of WidgetMetric objects	Metric list. Array Length: 1 - 200
title	No	String	Graph name. Minimum: 1 Maximum: 128 Regex Pattern: <code>^([\u4E00-\u9FFF] [a-z][A-Z][0-9] _ - : ; \\(\\) \\. \\~ ())+\$</code>
threshold	No	Double	Threshold of metrics on the graph. Minimum: 0 Maximum: 1.7976931348623157E308
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	Monitoring view chart type. The options are bar , line , bar_chart , table , circular_bar , and area_chart . Enumeration values: <ul style="list-style-type: none"> ● bar ● line ● bar_chart ● table ● circular_bar ● area_chart

Parameter	Mandatory	Type	Description
metric_display_mode	No	String	Metric display mode. The value can be single or multiple . Enumeration values: <ul style="list-style-type: none"> • single • multiple
properties	No	properties object	Graph display configuration.
location	No	location object	Graph coordinates.
unit	No	String	Unit.

Table 6-406 WidgetMetric

Parameter	Mandatory	Type	Description
namespace	Yes	String	Cloud service dimension. Minimum: 3 Maximum: 32 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. Minimum: 1 Maximum: 96 Regex Pattern: ^([A-Za-z]){1}([0-9A-Za-z] _ -)*\$
alias	No	Array of strings	Alias list of metrics on the graph. Minimum: 1 Maximum: 128 Array Length: 0 - 200
extra_info	No	ExtraInfo object	Metric information.

Table 6-407 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 . Minimum: 1 Maximum: 131 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}\$
filter_type	Yes	String	Resource type. The value can be all_instances (all resources) or specific_instances (specified resources). Enumeration values: <ul style="list-style-type: none"> • all_instances • specific_instances
values	No	Array of strings	Dimension value list. Minimum: 1 Maximum: 1024 Array Length: 0 - 200

Table 6-408 ExtraInfo

Parameter	Mandatory	Type	Description
origin_metric_name	Yes	String	Metric name. Minimum: 1 Maximum: 4096 Regex Pattern: ^([a-z] [A-Z] [0-9] _ ~ \. / :)*\$
metric_prefix	No	String	Metric name prefix. Minimum: 1 Maximum: 4096 Regex Pattern: ^([a-z] [A-Z] [0-9] _ ~ \. / :)*\$

Parameter	Mandatory	Type	Description
metric_type	No	String	Metric type. Minimum: 1 Maximum: 32 Regex Pattern: ^([a-z] [A-Z] [0-9] _ ~ \. / :)*\$
custom_proc_name	No	String	Custom process name. Minimum: 1 Maximum: 250

Table 6-409 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: <ul style="list-style-type: none"> • 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. Minimum: 1 Maximum: 2147483647 Default: 100
order	No	String	Sorting field. The value can be asc (ascending order) or desc (descending order). The line chart does not support this parameter. Enumeration values: <ul style="list-style-type: none"> • asc • desc

Table 6-410 location

Parameter	Mandatory	Type	Description
top	Yes	Integer	Grids between the graph and the top of the dashboard. Minimum: 0 Maximum: 2147483647
left	Yes	Integer	Grids between the graph and the left side of the dashboard. Minimum: 0 Maximum: 9
width	Yes	Integer	Graph width. Minimum: 3 Maximum: 12
height	Yes	Integer	Graph height. Minimum: 3 Maximum: 2147483647

Response Parameters

Status code: 200

Table 6-411 Response body parameters

Parameter	Type	Description
widgets	Array of BatchUpdateWidgetInfo objects	Update result list. Array Length: 1 - 50

Table 6-412 BatchUpdateWidgetInfo

Parameter	Type	Description
widget_id	String	Graph ID. Regex Pattern: ^wg([a-z] [A-Z] [0-9]){2}\$
ret_status	String	Update result. The value can be successful or error . Enumeration values: <ul style="list-style-type: none"> • successful • error

Parameter	Type	Description
error_msg	String	Error message when an operation fails. Minimum: 1 Maximum: 2048

Status code: 400

Table 6-413 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 401

Table 6-414 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-415 Response body parameters

Parameter	Type	Description
error_code	String	Status codes customized by each cloud service when a request error occurs. Minimum: 0 Maximum: 256
error_msg	String	Request error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Example Requests

```
[ {
  "widget_id" : "wgXXXXXXXXXXXXXXXXXXXX",
  "metrics" : [ {
    "namespace" : "SYS.ECS",
    "dimensions" : {
      "name" : "instance_id",
      "filter_type" : "specific_instances",
      "values" : [ "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" ],
      "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" : "view",
  "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" : "wgXXXXXXXXXXXXXXXXXXXX",
    "ret_status" : "successful"
  }, {
    "widget_id" : "wg9876543210123456789012",
    "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 Tags

6.14.1 Querying Tags of a Type of Resources in a Cloud Eye Project

Function

Querying tags of a type of resources in a Cloud Eye project.

URI

GET /v2/{project_id}/{resource_type}/tags

Table 6-416 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: 1 Maximum: 64 Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>
resource_type	Yes	String	Resource type. The options include: CES-alarm (alarm rule), CES-dashboard (dashboard), CES-resourceGroup (resource group), and CES-qualityMonitor (quality monitoring) Minimum: 1 Maximum: 32 Enumeration values: <ul style="list-style-type: none"> • CES-alarm • CES-dashboard • CES-resourceGroup • CES-qualityMonitor

Request Parameters

Table 6-417 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	No	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	Specifies the user token. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-418 Response body parameters

Parameter	Type	Description
tags	Array of Tag objects	Specifies tenant tags. Array Length: 0 - 20

Table 6-419 Tag

Parameter	Type	Description
key	String	Specifies a tag key. A tag key can contain up to 128 Unicode characters. key must be specified. Minimum: 0 Maximum: 128
values	Array of strings	Specifies tag values. Each value can contain up to 255 Unicode characters. If values is not specified, any parameter value can be queried. Minimum: 0 Maximum: 255 Array Length: 0 - 20

Status code: 404

Table 6-420 Response body parameters

Parameter	Type	Description
http_code	Integer	Specifies the HTTP status code. 200: OK 404: Resource not found. Minimum: 3 Maximum: 3 Enumeration values: <ul style="list-style-type: none"> • 200 • 404
message	GoAPIErrorResponseMsg object	Specifies the error message.

Table 6-421 GoAPIErrorResponseMsg

Parameter	Type	Description
details	String	Specifies the error message. Minimum: 0 Maximum: 1024
code	String	Specifies the service error codes. Minimum: 1 Maximum: 16

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 Server Monitoring Metrics from Different Dimensions

Function

This API is used to query metrics based on the ECS or BMS ID and from the following dimensions: disk, mount point, process, graphics card, and RAID controller. The NPU dimension is the original value, so there's no need to call this API to obtain the metric.

URI

GET /v2/{project_id}/instances/{instance_id}/agent-dimensions

Table 6-422 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID. Minimum: 1 Maximum: 64
instance_id	Yes	String	Resource ID, for example, 4270ff17-aba3-4138-89fa-820594c39755 . Minimum: 36 Maximum: 36

Table 6-423 Query Parameters

Parameter	Mandatory	Type	Description
dim_name	Yes	String	Dimension name. The options are as follows: mount_point indicates a mount point. disk indicates a disk. proc indicates a process. gpu indicates a graphics card. raid indicates a RAID controller. Enumeration values: <ul style="list-style-type: none"> • mount_point • disk • proc • gpu • raid

Parameter	Mandatory	Type	Description
dim_value	No	String	Dimension value, which contains 32 characters, for example, 2e84018fc8b4484b94e89aae212fe615 . Minimum: 32 Maximum: 32
offset	No	Integer	Pagination offset. Minimum: 0 Maximum: 2147483647 Default: 0 Regex Pattern: <code>^(0 [1-9][0-9]*)\$</code>
limit	No	Integer	Pagination size. Minimum: 1 Maximum: 1000 Default: 1000 Regex Pattern: <code>^([1-9] [1-9][0-9] [1-9][0-9][0-9] 1000)\$</code>

Request Parameters

Table 6-424 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	String	User token. Minimum: 1 Maximum: 16384

Response Parameters

Status code: 200

Table 6-425 Response body parameters

Parameter	Type	Description
dimensions	Array of AgentDimension objects	Dimension information. Array Length: 0 - 2147483647
count	Integer	Total number of dimensions. Minimum: 0 Maximum: 2147483647

Table 6-426 AgentDimension

Parameter	Type	Description
name	String	Dimension name. The options are as follows: mount_point indicates a mount point. disk indicates a disk. proc indicates a process. gpu indicates a graphics card. raid indicates a RAID controller. Enumeration values: <ul style="list-style-type: none"> • mount_point • disk • proc • gpu • raid
value	String	Dimension value, which contains 32 characters, for example, 2e84018fc8b4484b94e89aae212fe615 . Minimum: 32 Maximum: 32
origin_value	String	Actual dimension information. The value is a character string, for example, vda . Minimum: 1 Maximum: 1024

Status code: 400

Table 6-427 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: 0 Maximum: 256
error_msg	String	Error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 404

Table 6-428 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: 0 Maximum: 256
error_msg	String	Error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Status code: 500

Table 6-429 Response body parameters

Parameter	Type	Description
error_code	String	Error code. Minimum: 0 Maximum: 256

Parameter	Type	Description
error_msg	String	Error message. Minimum: 0 Maximum: 256
request_id	String	Request ID. Minimum: 0 Maximum: 256

Example Requests

This API is used to query metrics collected by Agent from a server whose **instance_id** is **4270ff17-aba3-4138-89fa-820594c39755**.

```
/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	Failed to verify parameters.
404	Page not found.
500	Failed to complete the request because of an internal server 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.

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 Regex Pattern: <code>^[a-z0-9]+\$</code>

Request Parameters

Table 7-2 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	String	Specifies the MIME type of the request body. The default type is application/json; charset=UTF-8 . Default: application/json; charset=UTF-8 Minimum: 1 Maximum: 64
X-Auth-Token	Yes	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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <code>^[a-zA-Z0-9-]{1,64}\$</code>

Parameter	Type	Description
uniagent_status	String	Specifies the uniagent status. The value can be none (not installed), running , silent , or unknown (faulty). Enumeration values: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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: <code>^(ces\.[0-9]{4})\$</code>
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: <code>^(ces\.[0-9]{4})\$</code>
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: <code>^(ces\.[0-9]{4})\$</code>
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: <code>^(ces\.[0-9]{4})\$</code>

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

This API is not supported at the following regions: LA-Buenos Aires1, and LA-Lima1.

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 Regex Pattern: <code>^[a-z0-9]+\$</code>

Table 7-12 Query Parameters

Parameter	Mandatory	Type	Description
instance_id	No	String	Specifies the server ID. Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>
instance_type	No	String	Specifies the server type. The value can be ECS or BMS . Enumeration values: <ul style="list-style-type: none"> • ECS • BMS
invocation_id	No	String	Specifies the task ID. Regex Pattern: <code>^([0-9A-Za-z]){1}([0-9A-Za-z] _ -)*\$</code>

Parameter	Mandatory	Type	Description
invocation_type	No	String	Specifies the task type, which can be INSTALL , UPDATE , or ROLLBACK . Enumeration values: <ul style="list-style-type: none"> • INSTALL • UPDATE • ROLLBACK • RETRY
invocation_target	No	String	Specifies the task object. Only telescope is supported. Default: telescope Enumeration values: <ul style="list-style-type: none"> • telescope
offset	No	Long	Specifies the pagination offset. Minimum: 0 Maximum: 999999999999999 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
X-Auth-Token	Yes	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: 999999999999999

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: <ul style="list-style-type: none"> • 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

Parameter	Type	Description
invocation_type	String	Specifies the task type, which can be INSTALL , UPDATE , or ROLLBACK . Enumeration values: <ul style="list-style-type: none"> ● 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: <ul style="list-style-type: none"> ● PENDING ● RUNNING ● TIMEOUT ● FAILED ● SUCCEEDED ● CANCELED ● ROLLBACKED
invocation_target	String	Specifies the task object. Only telescope is supported. Enumeration values: <ul style="list-style-type: none"> ● telescope
create_time	Long	Specifies when the task was created. Minimum: 11111111111111 Maximum: 99999999999999
update_time	Long	Specifies when the task was updated. Minimum: 11111111111111 Maximum: 99999999999999
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

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})\$

Parameter	Type	Description
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": "xxx",
    "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
  } ],
  "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

This API is not supported at the following regions: LA-Buenos Aires1, and LA-Lima1.

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 Regex Pattern: <code>^[a-z0-9]+\$</code>

Request Parameters

Table 7-21 Request header parameters

Parameter	Mandatory	Type	Description
Content-Type	Yes	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

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	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
invocation_type	Yes	String	Specifies the task type, which can be INSTALL , UPDATE , ROLLBACK , or RETRY . Enumeration values: <ul style="list-style-type: none"> • INSTALL • UPDATE • ROLLBACK • RETRY
invocation_target	No	String	Specifies the task object. Only telescope is supported. Default: telescope Enumeration values: <ul style="list-style-type: none"> • 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

Parameter	Mandatory	Type	Description
version_type	No	String	Specifies the version the Agent will be upgraded to. The value can be BASIC_VERSION or ADVANCE_VERSION . Enumeration values: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • CES • APICOM_BMS • ADMIN_SERVER
version	No	String	Version Number Minimum: 0 Maximum: 64 Regex Pattern: ^([0-9A-Za-z] \. \\. \\.)+\$

Response Parameters

Status code: 201

Table 7-23 Response body parameters

Parameter	Type	Description
invocations	Array of BatchCreateInvocationInfo objects	Specifies the information list of the created task. Array Length: 0 - 100

Table 7-24 BatchCreateInvocationInfo

Parameter	Type	Description
instance_id	String	Specifies the server ID. Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>
ret_status	String	Specifies the task result. The value can be successful or error . Enumeration values: <ul style="list-style-type: none"> • successful • error
error_msg	String	Specifies the error message. Minimum: 1 Maximum: 128
invocation_id	String	Specifies the task ID. Regex Pattern: <code>^[a-zA-Z0-9-]{1,64}\$</code>
error_code	String	Specifies the error code. Regex Pattern: <code>^(invocationmgr\.[0-9]{4})\$</code>

Status code: 400

Table 7-25 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the error code. Regex Pattern: <code>^(taskmgr\.[0-9]{4})\$</code>
error_msg	String	Specifies the error message. Minimum: 1 Maximum: 256

Status code: 401

Table 7-26 Response body parameters

Parameter	Type	Description
error_code	String	Specifies the error code. Regex Pattern: <code>^(taskmgr\.[0-9]{4})\$</code>

Parameter	Type	Description
error_msg	String	Specifies the error message. Minimum: 1 Maximum: 256

Status code: 403

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: 500

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

Example Requests

```
{
  "instance_ids" : [ "instancexx001", "instancexx002" ],
  "invocation_type" : "INSTALL",
  "invocation_target" : "telescope"
}
```

Example Responses

Status code: 201

Created

```
[ {
  "instance_id" : "instancexx001",
```

```
"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 permissions to call all APIs. An IAM user under the account can call specific APIs only after being 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.
- **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:li st	√	×

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.

Example Response

```
{
  "http_code": "403",
  "message": {
    "details": "Policy doesn't allow [ces:alarmHistoriesReportJob:create] to be performed",
    "code": "403"
  }
}
```

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 .

Glossary	Description
Metric	A metric consists of the namespace, dimension (optional), and metric name. A metric name solely does not identify any object.

Error Code Description

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.
	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.

Module	HTTP Status Code	Error Code	Error Code Description	Error Message	Measure
	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.
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.

Module	HTTP Status Code	Error Code	Error Code Description	Error Message	Measure
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.

A Appendix

A.1 Services Interconnected with Cloud Eye

Category	Service	Namespace	Dimension
Compute	Elastic Cloud Server	SYS.ECS	Key: instance_id Value: ECS ID
	ECS (OS monitoring)	AGT.ECS	Key: instance_id Value: ECS ID
	Bare Metal Server	SERVICE.BMS	Key: instance_id Value: BMS ID
	Auto Scaling	SYS.AS	Key: AutoScalingGroup Value: auto scaling group ID
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.)
	Object Storage Service	SYS.OBS	Key: bucket_name Value: bucket name
	Scalable File Service	SYS.SFS	Key: share_id Value: file system name
	SFS Turbo	SYS.EFS	Key: efs_instance_id Value: instance

Category	Service	Namespace	Dimension
Network	Elastic IP and bandwidth	SYS.VPC	<ul style="list-style-type: none"> Key: publicip_id Value: EIP ID Key: bandwidth_id Value: bandwidth ID
	Elastic Load Balance	SYS.ELB	<ul style="list-style-type: none"> Key: lb_instance_id Value: ID of a classic load balancer Key: lbaas_instance_id Value: ID of a shared load balancer Key: lbaas_listener_id Value: ID of a shared load balancer listener
	NAT Gateway	SYS.NAT	Key: nat_gateway_id Value: NAT gateway ID
	Virtual Private Network	SYS.VPN	Key: connection_id Value: VPN connection
	Cloud Connect	SYS.CC	<ul style="list-style-type: none"> Key: cloud_connect_id Value: cloud connection ID Key: bwp_id Value: bandwidth package ID Key: region_bandwidth_id Value: inter-region bandwidth ID
	Direct Connect	SYS.DCAAS	<ul style="list-style-type: none"> Key: direct_connect_id Value: connection Key: history_direct_connect_id Value: historical connection
	Global Accelerator	SYS.GA	<ul style="list-style-type: none"> Key: ga_accelerator_id Value: ID of the global accelerator Key: ga_listener_id Value: ID of a listener added to the global accelerator

Category	Service	Namespace	Dimension
Middleware	Distributed Message Service	SYS.DMS	For details, see the information in the right column.
	Distributed Cache Service	SYS.DCS	<ul style="list-style-type: none"> • 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
Database	Relational Database Service	SYS.RDS	For details, see the information in the right column.
	Document Database Service	SYS.DDS	<ul style="list-style-type: none"> • Key: mongodb_node_id Value: DDS node ID • Key: mongodb_instance_id Value: DDS DB instance ID
	GaussDB	SYS.NoSQL	For details, see the information in the right column.

Category	Service	Namespace	Dimension
	GaussDB(for MySQL)	SYS.GAUSSDB	<ul style="list-style-type: none"> • Key: gaussdb_mysql_instance_id Value: GaussDB(for MySQL) instance ID • Key: gaussdb_mysql_node_id Value: GaussDB(for MySQL) instance ID • Key: dbproxy_instance_id Value: GaussDB(for MySQL) Proxy instance ID • Key: dbproxy_node_id Value: GaussDB(for MySQL) Proxy node ID
	GaussDB	SYS.GAUSSDBV5	<ul style="list-style-type: none"> • Key: gaussdbv5_instance_id Value: GaussDB instance ID • Key: gaussdbv5_node_id Value: GaussDB node ID • Key: gaussdbv5_component_id Value: GaussDB component ID
Enterprise Intelligence	Cloud Search Service	SYS.ES	Key: cluster_id Value: CSS cluster
	ModelArts	SYS.ModelArts	<ul style="list-style-type: none"> • Key: service_id Value: real-time service ID • Key: model_id Value: model ID
	Data Lake Insight	SYS.DLI	<ul style="list-style-type: none"> • Key: queue_id Value: queue instance • Key: flink_job_id Value: Flink job

Category	Service	Namespace	Dimension
Security	Web Application Firewall	SYS.WAF	<ul style="list-style-type: none"> Key: instance_id Value: dedicated WAF instance Key: waf_instance_id Value: cloud WAF instance
	Database Security Service	SYS.DBSS	Key: audit_id Value: instance

A.2 Events Supported by Event Monitoring

Table A-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.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU link fault	GPULinkFault	Critical	The GPU of the host on which the ECS is located was faulty or was recovering from a fault.	Deploy service applications in HA mode. After the GPU fault is rectified, check whether services are restored.	Services are interrupted.
	ECS deleted	deleteServer	Major	The ECS was deleted <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> on the management console. by calling APIs. 	Check whether the restart was performed intentionally by a user. <ul style="list-style-type: none"> 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	<p>The ECS was stopped</p> <ul style="list-style-type: none"> • on the management console. • by calling APIs. <p>NOTE The ECS is stopped only after CTS is enabled.</p>	<ul style="list-style-type: none"> • 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	delete Nic	Major	The ECS NIC was deleted <ul style="list-style-type: none"> • on the management console. • by calling APIs. 	<ul style="list-style-type: none"> • 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	<p>The ECS specifications were resized</p> <ul style="list-style-type: none"> on the management console. by calling APIs. 	<ul style="list-style-type: none"> 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	Restart GuestOS	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 GPU memory is faulty, and services exit abnormally.
	FPGA link fault	FPGALinkFault	Critical	The FPGA of the host on which the ECS is located was <ul style="list-style-type: none"> faulty. 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
	Local disk replacement to be executed	localdisk_recovery_scheduled	Major	Local disk failure	Check the impact on services during the execution window.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Xid event alarm generated on GPU	commonXidError	Major	A xid event alarm occurs on GPU.	If services are affected, submit a service ticket.	The GPU hardware, driver, and application problems lead to Xid events, which may lead to abnormal exit of the business.
	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 disk failure	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.

 NOTE

Once a physical host running ECSs breaks down, the ECSs are automatically migrated to a functional physical host. During the migration, the ECSs will be restarted.

Table A-2 Bare Metal Server (BMS)

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
BMS	SYS.BMS	ECC uncorrectable error alarm generated on GPU SRAM	SRAM Uncorrectable EccError	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 GPU memory is faulty, and services exit abnormally.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		BMS restarted	osReboot	Major	<p>The BMS was restarted</p> <ul style="list-style-type: none"> on the management console. by calling APIs. 	<ul style="list-style-type: none"> Deploy service applications in HA mode. After the BMS is restarted, check whether services recover. 	Services are interrupted.
		Unexpected restart	serverReboot	Major	<p>The BMS restarted unexpectedly, which may be caused by</p> <ul style="list-style-type: none"> OS faults. hardware faults. 	<ul style="list-style-type: none"> 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 stopped	osShutdown	Major	The BMS was stopped <ul style="list-style-type: none"> on the management console. by calling APIs. 	<ul style="list-style-type: none"> Deploy service applications in HA mode. After the BMS is started, check whether services recover. 	Services are interrupted.
		Unexpected shutdown	serverShutdown	Major	The BMS was stopped unexpectedly, which may be caused by <ul style="list-style-type: none"> unexpected power-off. hardware faults. 	<ul style="list-style-type: none"> Deploy service applications in HA mode. After the BMS is started, check whether services recover. 	Services are interrupted.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Network disconnection	linkDown	Major	<p>The BMS network was disconnected . Possible causes are as follows:</p> <ul style="list-style-type: none"> • The BMS was unexpectedly stopped or restarted. • The switch was faulty. • The gateway was faulty. 	<ul style="list-style-type: none"> • Deploy service applications in HA mode. • After the BMS is started , check whether services recover . 	Services are interrupted.
		PCIe error	pcieError	Major	<p>The PCIe devices or main board of the BMS was faulty.</p>	<ul style="list-style-type: none"> • Deploy service applications in HA mode. • After the BMS is started , check whether services recover . 	The network or disk read/write services are affected.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Disk fault	diskError	Major	The disk backplane or disks of the BMS were faulty.	<ul style="list-style-type: none"> • 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.
		EVS error	storage Error	Major	<p>The BMS failed to connect to EVS disks. Possible causes are as follows:</p> <ul style="list-style-type: none"> • The SDI card was faulty. • Remote storage devices were faulty. 	<ul style="list-style-type: none"> • 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	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Inforom alarm generated on GPU	gpuInfoROM Alarm	Major	The driver failed to read inforom information due to GPU faults.	Non-critical services can continue to use the GPU card. For critical services, submit a service ticket to resolve this issue.	Services will not be affected if inforom information cannot be read. If error correction code (ECC) errors are reported on GPU, faulty pages may not be automatically retired and services are affected.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Double-bit ECC alarm generated on GPU	doubleBitEccError	Major	A double-bit ECC error occurred on GPU.	<ol style="list-style-type: none"> If services are interrupted, restart the services to restore. If services cannot be restarted, restart the VM where services are running. If services still cannot be restored, submit a service ticket. 	Services may be interrupted. After faulty pages are retired, the GPU card can continue to be used.
		Too many retired pages	gpuTooManyRetiredPagesAlarm	Major	An ECC page retirement error occurred on GPU.	If services are affected, submit a service ticket.	Services may be affected.

Event Source	Name Space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		ECC alarm generated on GPU Ant1	gpuAnt1EccAlarm	Major	An ECC error occurred on GPU.	<ol style="list-style-type: none"> 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 card can continue to be used.

Event Source	Name space	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.	<ol style="list-style-type: none"> 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 card.

Event Source	Name Space	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.	<ol style="list-style-type: none"> 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. 	Generally, this alarm is generated together with the ECC error alarm. If this alarm is generated independently, services are not affected.

Event Source	Name space	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 ECC errors.	<ol style="list-style-type: none"> 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 the NVIDIA driver cannot find the GPU card.	<ol style="list-style-type: none"> Restart the VM to restore services. If services still cannot be restored, submit a service ticket. 	The GPU card 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 GPU.
		GPU card lost	vmLostGpuAlarm	Major	The number of GPU cards on the VM is less than the number specified in the specifications.	If services are affected, submit a service ticket.	GPU cards get lost.

Event Source	Name space	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	Name space	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	Name Space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		System maintenance canceled	system_maintenance_cancelled	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	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GPU Xid error	commonXidError	Major	An Xid event alarm is generated on the GPU.	If services are affected, submit a service ticket.	An Xid error is caused by GPU hardware, driver, or application problems, which may result in abnormal service exit.
		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	PCleErrorFound	Major	The lspci command returns revff 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.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		NPU: request for restart AI process	Restart AIProcess	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.
		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 <i>Black Box Error Code Information List</i> and <i>Health Management Error Definition</i> .	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.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Table A-3 Elastic IP (EIP)

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
EIP	SYS.EIP	EIP bandwidth exceeded	EIPBandwidthOverflow	Major	<p>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.</p> <p>The metrics are described as follows:</p> <p>egressDropBandwidth: dropped outbound packets (bytes)</p> <p>egressAcceptBandwidth: accepted outbound packets (bytes)</p> <p>egressMaxBandwidthPerSec: peak outbound bandwidth (byte/s)</p> <p>ingressAcceptBandwidth: accepted</p>	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)		
		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.
		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

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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	<p>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.</p> <p>egressDropBandwidth: dropped outbound packets (bytes)</p> <p>egressAcceptBandwidth: accepted outbound packets (bytes)</p> <p>egressMaxBandwidthPerSec: peak outbound bandwidth (byte/s)</p> <p>ingressAcceptBandwidth: accepted inbound packets (bytes)</p> <p>ingressMaxBandwidthPerSec: peak inbound</p>	<p>Check whether the EIP bandwidth keeps increasing and whether services are normal. Increase bandwidth if necessary.</p>	<p>The network becomes slow or packets are lost.</p>

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
					bandwidth (byte/s) ingressDropBandwidth: dropped inbound packets (bytes)		

Table A-4 Advanced Anti-DDoS (AAD)

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
AAD	SYS.DDOS	DDoS Attack Events	ddos AttackEvents	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.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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 A-5 Elastic Load Balance (ELB)

Event Source	Name space	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 A-6 Cloud Backup and Recovery (CBR)

Event Source	Name space	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	Name space	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 A-7 Relational Database Service (RDS) — operations

Event Source	Name space	Event Name	Event ID	Event Severity	Description
RDS	SYS.RDS	Reset administrator password	resetPassword	Major	The password of the database administrator is reset.
		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 A-8 Document Database Service (DDS)

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
DDS	SYS .DDS	DB instance creation failure	DDSCreatelInstanceFailed	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	DDSA bnormalR eplica tionSt atus	Major	<p>The possible causes are as follows:</p> <p>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.</p> <p>The network between the primary instance and the standby instance or a read replica is disconnected.</p>	Submit a service ticket.	Your applications are not affected because this event does not interrupt data read and write.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Replication recovered	DDSR eplicationStatusRecovered	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	DDSF aulty DBInstance	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	DDS DBInstanceRecovered	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	DDSPPrimaryStandbySwitched	Major	A primary/standby switchover is performed or a failover is triggered.	No action is required.	None
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Data disk expanded and being writable	DDS Data DiskUsageRecovered	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	DDSPlanDeleteKMSKey	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.

Table A-9 GaussDB NoSQL

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB NoSQL	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	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Specifications modification failed	NoSQL ResizeInstanceFailed	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	NoSQL AddNodesFailed	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	NoSQL DeleteNodesFailed	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	NoSQL ScaleUpStorageFailed	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	NoSQL ResetPasswordFailed	Major	Resetting the password times out.	Reset the password again.	None
		Parameter group change failed	NoSQL UpdateInstanceParameterGroupFailed	Major	Changing a parameter group times out.	Change the parameter group again.	None
		Backup policy configuration failed	NoSQL SetBackupPolicyFailed	Major	The database connection is abnormal.	Configure the backup policy again.	None
		Manual backup creation failed	NoSQL CreateManualBackupFailed	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	NoSQL CreateAutomatedBackupFailed	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	NoSQL Faulty DBInstance	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	NoSQL DBInstanceRecovered	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	NoSQL Faulty DBNode	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	NoSQL DBNodeRecovered	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	NoSQL PrimaryStandbySwitched	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.	<ol style="list-style-type: none"> 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	BigKey Occurs	Major	The primary key design is improper. The number of records or data in a single partition is too large, causing unbalanced node loads.	<ol style="list-style-type: none"> 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	NoSQL RiskyDataDiskUsage	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	NoSQL DataDiskUsageRecovered	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	NoSQL CreateIndexFailed	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	NoSQL StallingOccurs	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	NoSQL StoppingOccurs	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.	<ol style="list-style-type: none"> 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	NoSQL Restart DBFailed	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	NoSQL RestoreToNewInstanceFailed	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	NoSQL RestoreToExistingInstanceFailed	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	NoSQL DeleteBackupFailed	Major	The backup files fail to be deleted from OBS.	Delete the backup files again.	None
		Failed to enable Show Original Log	NoSQL SwitchSlowlogPlainTextFailed	Major	The DB engine does not support this function.	Refer to the <i>GaussDB NoSQL User Guide</i> to ensure that the DB engine supports Show Original Log. Submit a service ticket to the O&M personnel.	None
		EIP binding failed	NoSQL BindEipFailed	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	NoSQL UnbindEipFailed	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	NoSQL ModifyParameterFailed	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	NoSQL ApplyParameterGroupFailed	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	NoSQL SwitchSSLFailed	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.	<p>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.</p> <p>2. Check whether there are invalid writes or encoding resulting in large keys or values.</p>	If there are rows that are too large, the cluster performance will deteriorate as the data volume grows.
		Schedule for deleting a KMS key	NoSQLplanDeleteKmsKey	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.	<ol style="list-style-type: none"> 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.

Table A-10 GaussDB(for MySQL)

Event Source	Name space	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	Taurus DeleteReadOnlyNodeFailed	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	Taurus ResetInstancePasswordFailed	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	Taurus RestartInstanceFailed	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.	Backup 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.	Backup jobs fail.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Primary / standby failover	Taurus ActiveStandby Switched	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.	<ol style="list-style-type: none"> 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	NodeReadOnly Mode	Major	The database supports only query operations.	Submit a service ticket.	After the database becomes read-only, write operations cannot be processed.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Database read/write	NodeReadWrite Mode	Major	The database supports both write and read operations.	Submit a service ticket.	None.
		Instance DR switchover	DisasterSwitch Over	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	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Database process restarted	Taurus DatabaseProcessRestarted	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 A-11 GaussDB

Event Source	Name space	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	Other Abnormal Alarm	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.
		Faulty DB instance	TaurusInstanceRunningStatusAbnormal	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	TaurusInstanceRunningStatusRecovered	Major	GaussDB(openGauss) provides an HA tool for automated or manual rectification of faults. After the fault is rectified, this event is reported.	No further action is required.	None
		Faulty DB node	TaurusNodeRunningStatusAbnormal	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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		DB node recovered	TaurusNodeRunningStatusRecovered	Major	GaussDB(openGauss) provides an HA tool for automated or manual rectification of faults. After the fault is rectified, this event is reported.	No further action is required.	None
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Node adding failure	Gauss DBV5 ExpandClusterFailed	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
		Storage scale-up failure	Gauss DBV5 EnlargeVolumeFailed	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	Gauss DBV5 RestartInstanceFailed	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.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Full backup failure	Gauss DBV5 FullBackup Failed	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	Gauss DBV5 Differential BackupFailed	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	Gauss DBV5 DeleteBackupFailed	Major	This function does not need to be implemented.	N/A	N/A
		EIP binding failure	Gauss DBV5 BindEIPFailed	Major	The EIP is bound to another resource.	Submit a service ticket to the O&M personnel.	The instance cannot be accessed from the Internet.
		EIP unbinding failure	Gauss DBV5 UnbindEIPFailed	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	Gauss DBV5 ApplyParameterFailed	Major	Modifying a parameter template times out.	Modify the parameter template again.	None

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Parameter modification failure	GaussDBV5 UpdateInstanceParameterGroupFailed	Major	Modifying a parameter template times out.	Modify the parameter template again.	None
		Backup and restoration failure	GaussDBV5 RestoreFromBackupFailed	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.
		Failed to upgrade the hot patch	GaussDBV5 UpgradeHotfixFailed	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

Table A-12 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	createLogi cDbF ailed	Major	<p>The possible causes are as follows:</p> <ul style="list-style-type: none"> 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. 	<p>Check whether</p> <ul style="list-style-type: none"> 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 A-13 Cloud Phone Server

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
CPH	SYS.CPH	Server shutdown	cpHServerOsShutdown	Major	<p>The cloud phone server was stopped</p> <ul style="list-style-type: none"> on the management console. by calling APIs. 	<p>Deploy service applications in HA mode.</p> <p>After the fault is rectified, check whether services recover.</p>	Services are interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Server abnormal shutdown	cpshServerShutdown	Major	<p>The cloud phone server was stopped unexpectedly. Possible causes are as follows:</p> <ul style="list-style-type: none"> The cloud phone server was powered off unexpectedly. The cloud phone server was stopped due to hardware faults. 	<p>Deploy service applications in HA mode.</p> <p>After the fault is rectified, check whether services recover.</p>	Services are interrupted.
		Server reboot	cpshServerOsReboot	Major	<p>The cloud phone server was rebooted</p> <ul style="list-style-type: none"> on the management console. by calling APIs. 	<p>Deploy service applications in HA mode.</p> <p>After the fault is rectified, check whether services recover.</p>	Services are interrupted.
		Server abnormal reboot	cpshServerReboot	Major	<p>The cloud phone server was rebooted unexpectedly due to</p> <ul style="list-style-type: none"> OS faults. hardware faults. 	<p>Deploy service applications in HA mode.</p> <p>After the fault is rectified, check whether services recover.</p>	Services are interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Network disconnection	cp hS erv erli nk Do wn	Major	<p>The network where the cloud phone server was deployed was disconnected. Possible causes are as follows:</p> <ul style="list-style-type: none"> • The cloud phone server was stopped unexpectedly and rebooted. • The switch was faulty. • The gateway node was faulty. 	<p>Deploy service applications in HA mode.</p> <p>After the fault is rectified, check whether services recover.</p>	Services are interrupted.
		PCIe error	cp hS erv erP cie Error	Major	<p>The PCIe device or main board on the cloud phone server was faulty.</p>	<p>Deploy service applications in HA mode.</p> <p>After the fault is rectified, check whether services recover.</p>	The network or disk read/write is affected.
		Disk error	cp hS erv er DiskError	Major	<p>The disk on the cloud phone server was faulty due to</p> <ul style="list-style-type: none"> • disk backplane faults. • disk faults. 	<p>Deploy service applications in HA mode.</p> <p>After the fault is rectified, check whether services recover.</p>	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	cp hServerStorageError	Major	<p>The cloud phone server could not connect to EVS disks. Possible causes are as follows:</p> <ul style="list-style-type: none"> • SDI card faults • Remote storage devices were faulty. 	<p>Deploy service applications in HA mode.</p> <p>After the fault is rectified, check whether services recover.</p>	<p>Data read/write services are affected, or the BMS cannot be started.</p>
		GPU offline	cp hServerGpuOffline	Major	<p>GPU of the cloud phone server was loose and disconnected.</p>	<p>Stop the cloud phone server and reboot it.</p>	<p>Faults occur on cloud phones whose GPUs are disconnected. Cloud phones cannot run properly even if they are restarted or reconfigured.</p>

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		GPU timeout	cp hServer GpuTime Out	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	cp hServer DiskFull	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 read only	cp hServer DiskRead Only	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	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		Cloud phone metadata damaged	cp hP hone Me ta Da ta Da ma ge	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	gp uA bn or ma l	Critical	The GPU was faulty.	Submit a service ticket.	Services are interrupted.
		GPU recovered	gp uN or ma l	Informational	The GPU was running properly.	No further action is required.	N/A
		Kernel crash	ker nel Cra sh	Critical	The kernel log indicated crash.	Submit a service ticket.	Services are interrupted during the crash.
		Kernel OOM	ker nel Oom	Major	The kernel log indicated out of memory.	Submit a service ticket.	Services are interrupted.
		Hardware malfunction	har dw are Err or	Critical	The kernel log indicated Hardware Error .	Submit a service ticket.	Services are interrupted.
		PCIe error	pci eA er	Critical	The kernel log indicated PCIe Bus Error .	Submit a service ticket.	Services are interrupted.

Event Source	Name space	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 /.share dpath/master became read-only	isuladMasterReadOnly	Critical	Mount point /.share dpath/master of the image storage became read-only.	Submit a service ticket.	Services are interrupted.
		Cloud phone data disk became read-only	cp hDiskReadOnly	Critical	The cloud phone data disk became read-only.	Submit a service ticket.	Services are interrupted.
		Cloud phone data disk superblock damaged	cp hDiskBadSuperBlock	Critical	The superblock of the file system of the cloud phone data disk was damaged.	Submit a service ticket.	Services are interrupted.

Table A-14 Layer 2 Connection Gateway (L2CG)

Event Source	Name Space	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 A-15 Elastic IP and bandwidth

Event Source	Name Space	Event Name	Event ID	Event Severity
Elastic IP and bandwidth	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 A-16 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	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 A-17 Identity and Access Management (IAM)

Event Source	Name space	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 A-18 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 A-19 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 A-20 Cloud Eye

Event Source	Name Space	Event Name	Event ID	Event Severity	Description	Solution
Cloud Eye	SYS.CES	Agent heartbeat interruption	agentHeartbeatInterrupted	Major	The Agent sends a heartbeat message to Cloud Eye every minute. If Cloud Eye cannot receive a heartbeat for 3 minutes, Agent Status is displayed as Faulty .	<ul style="list-style-type: none"> • 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	Name space	Event Name	Event ID	Event Severity	Description	Solution
						<p>into the corresponding hosts file.</p> <ul style="list-style-type: none"> Update the Agent to the latest version.
		Agent back to normal	agentResumed	Informational	The Agent was back to normal.	No further action is required.
		Agent faulty	agentFaulty	Major	The Agent was faulty and this status was reported to Cloud Eye.	<p>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.</p> <p>Update the Agent to the latest version.</p>

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution
		Agent disconnected	agentDisconnected	Major	<p>The Agent sends a heartbeat message to Cloud Eye every minute. If Cloud Eye cannot receive a heartbeat for 3 minutes, Agent Status is displayed as Faulty.</p>	<p>Confirm that the Agent domain name cannot be resolved.</p> <p>Check whether your account is in arrears.</p> <p>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.</p> <p>Confirm that the server time is inconsistent with the local standard time.</p> <p>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.</p>

Table A-21 Enterprise Switch

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
Enterprise Switch	SYS.ESW	IP address 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 A-22 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	operateDeleteSecret	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 A-23 Distributed Cache Service (DCS)

Event Source	Name space	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.
		Automatic failover	masterStandbyFailover	Minor	The master node was abnormal, promoting a replica to master.	Check whether services can recover by themselves. If applications cannot recover, restart them.	Persistent connections to the instance are interrupted.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

Event Source	Namespace	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		Instance node abnormal restart	instanceNodeAbnormalRestart	Major	DCS nodes restarted unexpectedly when they became faulty.	Check whether services can recover. If the applications are not reconnected, 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 scripts to prevent execution timeout.	If Lua scripts take a long time to execute, they will be forcibly stopped to avoid blocking the entire instance.
		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.

Table A-24 Intelligent Cloud Access (ICA)

Event Source	Name space	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 A-25 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	Namespace	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 A-26 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
		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

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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
		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 A-27 Cloud Certificate Manager (CCM)

Event Source	Name space	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.
		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.

Event Source	Name space	Event Name	Event ID	Event Severity	Description	Solution	Impact
		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.
		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.

B Change History

Released On	Description
2025-01-30	This issue is the second official release, which incorporates the following changes: <ul style="list-style-type: none">• Added API V2.• Added API V3.
2022-09-30	This issue is the first official release.