Cloud Eye

API Reference

Issue	01
Date	2022-09-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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.

Contents

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 running 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 registration. 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
Cloud Eye API	API version management	**Querying All API Versions**	Query all API versions supported by Cloud Eye.
		Querying a Specified API Version	Query a specified API version supported by Cloud Eye.
	Metric management	**Querying the Metrics**	Query the list of metrics that currently monitored by Cloud Eye.
	Alarm rule management	**Querying the Alarm Rule List**	Query the alarm rule list.
		Querying an Alarm Rule	Query the alarm rule information based on the alarm rule 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 the alarm rule ID.
		Creating an Alarm Rule	Create an alarm rule.
	Monitoring data management	**Querying Monitoring Data**	Query the monitoring data of a specified metric of specified granularity in a specified time range.

Type	Subtype	API	Description
		Adding Monitoring Data	Add one or more pieces of metric monitoring data.
	Quota management	**Querying Quotas**	Query the alarm rule quota.
	Event monitoring	**Reporting Events**	Report custom events.

3 Calling APIs

3.1 Making an API Request

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

Request URI

A request URI is in the following format:

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

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

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 *Parameter name*=*Parameter value*. For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

For example, to obtain an IAM token in the **Dublin** region, obtain the endpoint of IAM (**iam.myhuaweicloud.eu**) for this region and the **resource-path** (**/v3/auth/tokens**) in the URI of the API used to **obtain a user token**. Then, construct the URI as follows:

```
https://iam.myhuaweicloud.eu/v3/auth/tokens
```

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 used to **obtain a user token**, the request method is **POST**. The request is as follows:

```
POST https://iam.myhuaweicloud.eu/v3/auth/tokens
```


Request Header

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

Common request header fields are as follows.

Table 3-3 Common request header fields

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

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

NOTE

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

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

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

```
POST https://iam.myhuaweicloud.eu/v3/auth/tokens
Content-Type: application/json
```

(Optional) Request Body

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

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

In the case of the API used to **obtain a user token**, the request parameters and parameter description can be obtained from the API request. The following provides an example request with a body included. Replace *username*, *domainname*, ******** (login password), and *xxxxxxxxxxxxxxxxx* (project name) with the actual values. Obtain a project name from Regions and Endpoints.

NOTE

The **scope** parameter specifies where a token takes effect. You can set **scope** to an account or a project under an account. In the following example, the token takes effect only for the resources in a specified project. For more information about this API, see **Obtaining a User Token**.

```
POST https://iam.myhuaweicloud.eu/v3/auth/tokens
Content-Type: application/json
```



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

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

3.2 Authentication

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

- Token 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.

A cloud service can be deployed as either a project-level service or global service.

- For a project-level service, you need to obtain a project-level token. When you call the API, set **auth.scope** in the request body to **project**.
- For a global service, you need to obtain a global token. When you call the API, set **auth.scope** in the request body to **domain**.

IMS 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",
                "password": "********",
                "domain": {
                    "name": "domainname"
                }
            }
        }
    },
    "scope": {
        "project": {
            "name": "xxxxxxxx"
        }
    }
  }
}
```

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

```
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 **obtain a user token**, the request is successful.

Response Header

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

Figure 3-1 shows the response header fields for the API used to **obtain a user token**. The **x-subject-token** header field is the desired user token. This token can then be used to authenticate the calling of other APIs.

Figure 3-1 Header fields of the response to the request for obtaining a user token

(Optional) Response Body

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

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

```
{
    "token": {
```



```
    "expires_at": "2019-02-13T06:52:13.855000Z",
    "methods": [
        "password"
    ],
    "catalog": [
        {
            "endpoints": [
                {
                    "region_id": "az-01",
.....
```

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 format of message is error",
    "error_code": "AS.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 invoke a number of 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.

Creation Procedure

1. **Obtain the user token.**
2. **Query the list of metrics that can be monitored.**
3. **Create an alarm rule.**

Procedure

1. Obtain the user token.

   Send **POST https://***IAM endpoint***/v3/auth/tokens**.

   Add **Content-Type:application/json** to the request headers.

   The request body is as follows:

```
{
  "auth": {
    "identity": {
      "methods": [
        "password"
      ],
      "password": {
        "user": {
          "name": "James",
          "password": "**********",
          "domain": {
            "name": "A-Company"
          }
        }
      }
    },
    "scope": {
      "project": {
        "name": "XXX",
```



```
      "domain": {
        "name": "A-Company"
      }
    }
  }
 }
}
```

Specify the following parameters:

- **user.name**: username, which is set based on the obtained token body
- **password**: login password
- **domain.name:**: name of the account to which the user belongs. If the account is used to obtain the token, values of **user.name** of the account and **domain.name** are the same. In this case, enter the **user.name** value. Otherwise, enter the domain name to which the account belongs.
- **project.name**: region

  For details about region names, see **Regions and Endpoints**.

  NOTE

  Obtain **X-Subject-Token** from the response header, that is, the signed token.

2. Query the list of metrics that can be monitored.

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

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

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

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

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

3. Create an alarm rule.

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

   Specify the following parameters in the request body:

```
{
  "alarm_name": "alarm-rp0E",  //Alarm rule name (mandatory, string)
  "alarm_description": "",
  "metric": {
    "namespace": "SYS.ECS",  //Namespace (mandatory, string)
    "dimensions": [
      {
        "name": "instance_id",
```

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

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

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

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

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

5 API Description

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 Metric Management

5.2.1 Querying the Metrics

Function

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

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	Query 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	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**.

Parameter	Mandatory	Type	Description
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.
order	No	String	Specifies the result sorting method, which is sorted by timestamp. The default method is **desc**. • **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.
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**.

Parameter	Type	Description
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.

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

Error Codes

See **Error Codes**.

5.3 Alarm Rule Management

5.3.1 Querying the Alarm Rule List

Function

This API is used to 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.

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**. • **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 Response parameters

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**.
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.

Parameter	Type	Description
alarm_state	String	Specifies the alarm status, which can be • **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	Query 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**.
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. • **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. • **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. The following methods are supported: • **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 **cpu_util** 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	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 5-24 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 **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**.
total	Integer	Specifies the total number of query results.

- Example response

```
{
    "metric_alarms": [
        {
            "alarm_name": "alarm-ttttttt",
            "alarm_description": "",
            "metric": {
                "namespace": "SYS.ECS",
                "dimensions": [
                    {
```



```
                "name": "instance_id",
                "value": "07814c0e-59a1-4fcd-a6fb-56f2f6923046"
            }
          ],
          "metric_name": "cpu_util"
       },
       "condition": {
          "period": 300,
          "filter": "average",
          "comparison_operator": ">=",
          "value": 0,
          "unit": "%",
          "count": 3
       },
       "alarm_enabled": true,
       "alarm_level": 2,
       "alarm_action_enabled": false,
       "alarm_id": "al15330507498596W7vmlGKL",
       "update_time": 1533050749992,
       "alarm_state": "alarm"
    },
    {
       "alarm_name": "alarm-m5rwxxxxxxx",
       "alarm_description": "",
       "metric": {
          "namespace": "SYS.ECS",
          "dimensions": [
             {
                "name": "instance_id",
                "value": "30f3858d-4377-4514-9081-be5bdbf1392e"
             }
          ],
          "metric_name": "network_incoming_bytes_aggregate_rate"
       },
       "condition": {
          "period": 300,
          "filter": "average",
          "comparison_operator": ">=",
          "value": 12,
          "unit": "Byte/s",
          "count": 3
       },
       "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	You are forbidden to access the page requested.
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 an Alarm Rule

Function

This API is used to query an alarm rule based on the alarm rule 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 • **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	Query 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 IID of the resource group 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. • **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. • **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. The following methods are supported: • **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 **cpu_util** 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	Specifies the interval for triggering an alarm if the alarm persists. Possible intervals are as follows: **0**: Cloud Eye triggers the alarm only once. **300**: Cloud Eye triggers the alarm every 5 minutes. **600**: Cloud Eye triggers the alarm every 10 minutes. **900**: Cloud Eye triggers the alarm every 15 minutes. **1800**: Cloud Eye triggers the alarm every 30 minutes. **3600**: Cloud Eye triggers the alarm every hour. **10800**: Cloud Eye triggers the alarm every 3 hours. **21600**: Cloud Eye triggers the alarm every 6 hours. **43200**: Cloud Eye triggers the alarm every 12 hours. **86400**: Cloud Eye triggers the alarm every day.

- Example 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
     },
   "alarm_enabled":true,
   "alarm_level": 2,
   "alarm_action_enabled":true,
   "alarm_actions":
    [
```



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

Returned Values

- Normal

  200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	You are forbidden to access the page requested.
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. • **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.

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

Error Codes

See **Error Codes**.

5.3.4 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	Arrays of objects	Specifies the action to be triggered by an alarm.
			An example structure is as follows:
			{
			"type": "notification","notificationList": ["urn:smn:region:68438a86d98e427e907e0097b7e35d47:sd"]
			}
			For details, see **Table 5-39**.

ok_actions	No	Arrays of objects	Specifies the action to be triggered after the alarm is cleared. Its structure is: { "type": "notification","notificationList": ["urn:smn:region:68438a86d98e427e907e0097b7e35d47:sd"] } For details, see **Table 5-40**.

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

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	Arrays 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 the 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	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. 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 5-39 alarm_actions data structure description

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

Parameter	Mandatory	Type	Description
notificationList	Yes	Arrays of strings	Specifies the list of objects to be notified if the alarm status changes. You can configure up to 5 object IDs. **topicUrn** can be obtained from SMN. For details, see **Querying Topics**. If you set **type** to **notification**, you must specify **notificationList**. If you set **type** to **autoscaling**, you must set **notificationList** to **[]**. **NOTE** • To 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	Specifies the notification type when an alarm is triggered. • **notification**: indicates that a notification will be sent. • **autoscaling**: indicates that a scaling action will be triggered.

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

Table 5-41 insufficientdata_actions data structure description

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

Table 5-42 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** • 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 operator of alarm thresholds. Possible operators are >, =, <, >=, and <=.
value	Yes	Double	Specifies the alarm threshold. Supported range: **0** to **Number. MAX_VALUE (1.7976931348623157e+108)** For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** in **Services Interconnected with Cloud Eye** to **80**.
unit	No	String	Specifies the data unit. Enter up to 32 characters.
count	Yes	Integer	Specifies the number of consecutive occurrence times that the alarm policy was met. Supported range: **1** to **5**

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

- Example request

```
{
   "alarm_name": "alarm-rp0E",
   "alarm_description": "",
   "metric": {
      "namespace": "SYS.ECS",
      "dimensions": [
         {
            "name": "instance_id",
            "value": "33328f02-3814-422e-b688-bfdba93d4051"
         }
      ],
      "metric_name": "network_outgoing_bytes_rate_inband"
   },
   "condition": {
      "period": 300,
      "filter": "average",
      "comparison_operator": ">=",
      "value": 6,
      "unit": "Byte/s",
      "count": 1
   },
   "alarm_enabled": true,
   "alarm_action_enabled": true,
   "alarm_level": 2,
   "alarm_actions": [
      {
         "type": "notification",
         "notificationList": ["urn:smn:region:68438a86d98e427e907e0097b7e35d48:sd"]
```



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

Response

- Response parameters

  Table 5-43 Response parameters

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.

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

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

- Example request

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



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

Response

- Response parameters

  Table 5-48 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 Alarm History

Function

This API is used to query alarm history 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). **from** must be less than or equal to **to**. 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	Specifies the action to be triggered by an alarm. The structure is as follows: {"type": "notification", "notificationList": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"] } The value of **type** can be one of the following: **notification**: indicates that a notification will be sent. **autoscaling**: indicates that a scaling action will be triggered. **notificationList**: indicates the list of objects to be notified if the alarm status changes. For details, see **Table 5-54**.
ok_actions	Array of objects	No	Specifies the action to be triggered after the alarm is cleared. The structure is as follows: {"type": "notification", "notificationList": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"] } The value of **type** can be one of the following: **notification**: indicates that a notification will be sent. **notificationList**: indicates the list of objects to be notified if the alarm status changes. For details, see **Table 5-55**.

Parameter	Type	Mandatory	Description
insufficientdata_actions	Array of objects	No	Specifies the action triggered by data insufficiency. The structure is as follows: {"type": "notification", "notificationList": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"]} The value of **type** can be one of the following: **notification**: An alarm is triggered due to insufficient data. **notificationList**: Specifies the ID list of the notification objects when an alarm notification is triggered due to insufficient data. For details, see **Table 5-56**.
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	Arrays of objects	Yes	Specifies the metric dimension. For details, see **Table 5-53**.
metric_name	String	Yes	Specifies the metric name. Start with a letter. Enter 1 to 64 characters. Only letters, digits, and underscores (_) are allowed. For details, see the metric name queried in **Services Interconnected with Cloud Eye**.
namespace	String	Yes	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. • **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. • **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. • **notification**: indicates that a notification will be sent. • **autoscaling**: indicates that a scaling action will be triggered.

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

Table 5-57 condition data structure description

Parameter	Type	Mandatory	Description
period	Integer	Yes	Specifies how often Cloud Eye aggregates data, which can be • **1**: Cloud Eye performs no aggregation and displays raw data. • **300**: Cloud Eye aggregates data every 5 minutes. • **1200**: Cloud Eye aggregates data every 20 minutes. • **3600**: Cloud Eye aggregates data every 1 hour. • **14400**: Cloud Eye aggregates data every 4 hours. • **86400**: Cloud Eye aggregates data every 24 hours. **NOTE** If you set **period** to **1**, Cloud Eye uses raw data to determine whether to trigger an alarm. You can set this parameter to **0** when you set **alarm_type** to **(EVENT.SYS| EVENT.CUSTOM)**.

Parameter	Type	Mandatory	Description
filter	String	Yes	Specifies the data rollup method, which can be • **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 operator of alarm thresholds, which can be >, =, <, >=, or <=.
value	Double	Yes	Specifies the alarm threshold. Supported range: **0** to **Number. MAX_VALUE (1.7976931348623157e+108)** For detailed thresholds, see the value range of each metric in the appendix. For example, you can set ECS **cpu_util** in **Services Interconnected with Cloud Eye** to **80**.
unit	String	No	Specifies the data unit. Enter up to 32 characters.
count	Integer	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. **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": "al1604473978613MvlvlbVZD",
    "alarm_name": "alarm_merge",
    "alarm_description": "",
    "metric": {
      "namespace": "AGT.ECS",
      "dimensions": [
        {
          "name": "instance_id",
          "value": "22d98f6c-16d2-4c2d-b424-50e79d82838f"
        }
      ],
      "metric_name": "load_average5",
      "resource_group_id": "rg16044739783733030 3XQbK",
      "resource_group_name": "group1"
    },
    "condition": {
      "period": 1,
      "filter": "average",
      "comparison_operator": ">=",
      "value": 0,
      "count": 3
    },
    "alarm_level": 2,
    "alarm_type": "RESOURCE_GROUP",
    "alarm_enabled": false,
    "alarm_action_enabled": false,
    "alarm_actions": [],
    "ok_actions": [],
    "insufficientdata_actions": [],
    "update_time": 1604473979000,
    "enterprise_project_id": "0",
    "trigger_time": 1604473979070,
    "alarm_status": "insufficient_data",
    "datapoints": [],
    "additional_info": {
      "resource_id": "",
      "resource_name": "",
      "event_id": ""
    }
  }
 ],
 "meta_data": {
   "total": 2
 }
}
```


Returned Values

- Normal

  200

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	You are forbidden to access the page requested.
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**.

Parameter	Type	Mandatory	Description
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 resource 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}/alarms/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	Mandatory	Description
metric_name	String	Yes	Specifies the metric you add to the custom alarm template. For example, you can add ECS **cpu_util**. To view metrics of each resource, see **Services Interconnected with Cloud Eye**.
condition	Condition object	Yes	Specifies the alarm policy you created for the custom alarm template. For details, see **Table 5-64**.
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	Mandatory	Description
period	Integer	Yes	Specifies how often Cloud Eye aggregates data. Possible values: • **1**: Cloud Eye performs no aggregation and displays raw data. • **300**: Cloud Eye aggregates data every 5 minutes. • **1200**: Cloud Eye aggregates data every 20 minutes. • **3600**: Cloud Eye aggregates data every 1 hour. • **14400**: Cloud Eye aggregates data every 4 hours. • **86400**: Cloud Eye aggregates data every 24 hours.
filter	String	Yes	Specifies the data rollup method. The following methods are supported: • **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.

Parameter	Type	Mandatory	Description
count	Integer	Yes	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 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.

Returned Value	Description
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, which can contain 1 to 128 characters. Only letters, digits, and underscores (_) are allowed.

Parameter	Mandatory	Type	Description
template_description	No	String	Provides supplementary information about the custom alarm template, which can contain 0 to 256 characters.
namespace	Yes	String	Specifies the resource type selected for creating the custom alarm template, that is, the service namespace. For example, if you select ECS, **namespace** is **SYS.ECS**.
dimension_name	Yes	String	Specifies the dimension corresponding to the resource type. If ECS is selected, the dimension is ECS and **dimension_name** is **instance_id**.
template_items	Yes	Arrays 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: • **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.
unit	No	String	Specifies the data unit, which can contain up to 32 characters.
value	Yes	Double	Specifies the alarm threshold. Supported range: **0** to **Number.MAX_VALUE (1.7976931348623157e+108)** For detailed thresholds, see the value range of each metric in **Services Interconnected with Cloud Eye**. For example, you can set ECS **cpu_util** to **80**.

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

- Example request

```
{
  "template_name": "alarmTemplate-Test01",
  "template_description": "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	Arrays of objects	Specifies the action to be triggered by an alarm. The structure example 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	Arrays 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	Arrays 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 • **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.
filter	Yes	String	Specifies the data rollup method, which can be • **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 operator of alarm thresholds, 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. • **notification**: indicates that a notification will be sent. • **autoscaling**: indicates that a scaling action will be triggered.

Parameter	Mandatory	Type	Description
notificationList	Yes	Arrays of strings	Specifies the list of objects to be notified if the alarm status changes. You can configure up to 5 object IDs. **topicUrn** can be obtained from SMN. For details, see **Querying Topics**. If you set **type** to **notification**, you must specify **notificationList**. If you set **type** to **autoscaling**, you must set **notificationList** to **[]**. **NOTE** • To 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	Specifies the notification type when an alarm is triggered. • **notification**: indicates that a notification will be sent. • **autoscaling**: indicates that a scaling action will be triggered.

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

Table 5-75 insufficientdata_actions data structure description

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

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

- Example request

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

Returned Values

- Normal

  204

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	You are forbidden to access the page requested.
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 Management

5.4.1 Querying Monitoring Data

Function

This API is used to 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.

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 the Metrics**.
from	Yes	String	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. Therefore, 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. Therefore, 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	Specifies how often Cloud Eye aggregates data, which can be • **1**: Cloud Eye performs no aggregation and displays raw data. • **300**: Cloud Eye aggregates data every 5 minutes. • **1200**: Cloud Eye aggregates data every 20 minutes. • **3600**: Cloud Eye aggregates data every 1 hour. • **14400**: Cloud Eye aggregates data every 4 hours. • **86400**: Cloud Eye aggregates data every 24 hours.
filter	Yes	String	Specifies the data rollup method, which can be • **average**: 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. **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.

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

NOTE

- **dimensions** can be obtained from the response body by calling the API for **Querying the 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 Response parameters

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	You are forbidden to access the page requested.
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.

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

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

- Request parameters

  Table 5-81 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: • **int** • **float**

Table 5-83 metric data structure description

Parameter	Mandatory	Type	Description
namespace	Yes	String	Specifies the customized namespace. 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 (_). In addition, **service** cannot start with **SYS** and **AGT**, and **namespace** cannot be **SERVICE.BMS** because this namespace has been used by the system. You can leave this parameter blank when you set **alarm_type** to **(EVENT.SYS| EVENT.CUSTOM)**.
dimensions	Yes	Array of objects	Specifies the metric dimension. A maximum of three dimensions are supported. For details, see **Table 5-84**.
metric_name	Yes	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 5-84 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.

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 the ECS whose **instance_id** is **6f3c6f91-4b24-4e1b-b7d1-a94ac1cb011d**.

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

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

```
[
  {
    "metric": {
      "namespace": "SYS.RDS",
      "dimensions": [
        {
          "name": "rds_cluster_id",
          "value": "3c8cc15614ab46f5b8743317555e0de2in01"
        }
      ],
      "metric_name": "rds021_myisam_buf_usage"
    },
```



```
    "ttl": 172800,
    "collect_time": 1463598260000,
    "type": "float",
    "value": 0.01,
    "unit": "Ratio"
  }
]
```

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

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

Response

The response has no message body.

Returned Values

- Normal

  201

- Abnormal

Returned Value	Description
400 Bad Request	Request error.
401 Unauthorized	The authentication information is not provided or is incorrect.
403 Forbidden	You are forbidden to access the page requested.
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 in Batches

Function

You can 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 500 metrics in batches.

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 60000 ms (60 x 1000).
   - If **period** is **300**, the monitoring interval is 300000 ms (300 x 1000).
   - If **period** is **1200**, the monitoring interval is 1200000 ms (1200 x 1000).
   - If **period** is **3600**, the monitoring interval is 3600000 ms (3600 x 1000).
   - If **period** is **14400**, the monitoring interval is 14400000 ms (14400 x 1000).
   - If **period** is **86400**, the monitoring interval is 86400000 ms (86400 x 1000).

   For example, if 300 metrics are queried in batches and the monitoring interval is 60000 ms, the maximum value of (**to**-**from**) is **600000**. If (**to-from**) exceeds 600000, **from** is automatically changed to **to-600000**.

- Request parameters

  Table 5-86 Request parameters

Parameter	Mandatory	Type	Description
metrics	Yes	Arrays 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	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. Therefore, 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. Therefore, 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	long	Specifies the end time of the query. The time is a UNIX timestamp and the unit is ms. **from** must be earlier than **to**.
period	Yes	String	Specifies how often Cloud Eye aggregates data, which can be • **1**: Cloud Eye performs no aggregation and displays raw data. • **300**: Cloud Eye aggregates data every 5 minutes. • **1200**: Cloud Eye aggregates data every 20 minutes. • **3600**: Cloud Eye aggregates data every 1 hour. • **14400**: Cloud Eye aggregates data every 4 hours. • **86400**: Cloud Eye aggregates data every 24 hours.

Parameter	Mandatory	Type	Description
filter	Yes	String	Specifies the data rollup method, which can be • **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. **filter** does not affect the query result of raw data. (The period is **1**.)

Table 5-87 metrics data structure description

Parameter	Mandatory	Type	Description
namespace	Yes	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	Yes	Arrays of objects	Specifies the list of the metric dimensions.
			Each dimension is a JSON object, and its structure is as follows:
			{
			"name": "instance_id",
			"value": "33328f02-3814-422e-b688-bfdba93d4050"
			}
			For details, see **Table 5-88**.

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

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. 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 the Metrics**.
- OBS metric data can be queried only when the related OBS APIs are called.

- Example request

  Request example 1: 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 2: 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 3: 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": "b28354b543375bfa94dabaeda722927"
            }
        ],
        "metric_name": "proc_specified_count"
    }
  ],
  "from": 1556625600000,
  "to": 1556632800000,
  "period": "1200",
  "filter": "min"
}
```

Response

- Response parameters

Table 5-89 Response parameters

Parameter	Type	Description
metrics	Arrays 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	Arrays of objects	Specifies the metric data list. Since Cloud Eye rounds up **from** based on the level of granularity for data query, **datapoints** may contain more data points than expected. 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	Arrays of objects	Specifies the list of metric dimensions.
		Each dimension is a JSON object, and its structure is as follows:
		{
		"name": "instance_id",
		"value": "33328f02-3814-422e-b688-bfdba93d4050"
		}
		For details, see **Table 5-91**.

Parameter	Type	Description
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 **proc_specified_count** 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.
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 Quota Management

5.5.1 Querying Quotas

Function

This API is used to query a resource quota and the used amount. The current resource refers to alarm rules only.

URI

GET /V1.0/{project_id}/quotas

- 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**.

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

Request

None

Response

- Response parameters

Table 5-94 Response parameters

Parameter	Type	Description
quotas	Object	Specifies the quota list. For details, see **Table 5-95**.

Table 5-95 Data structure description of **quotas**

Parameter	Type	Description
resources	Array of objects	Specifies the resource quota list. For details, see **Table 5-96**.

Table 5-96 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 Group Management

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 5-97 Parameter description

Parameter	Mandatory	Description
project_id	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
group_id	Yes	Specifies the resource group ID.
status	No	Specifies the resource group status, which can be **health**, **unhealth**, or **no_alarm_rule**. **health** indicates that no alarms have been generated for the resource group.
namespace	No	Specifies the resource namespace. For example, the resource namespace of an ECS 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 5-98 Response parameters

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	Arrays of objects	Specifies information about one or more resource groups. For details, see **Table 5-99**.
status	String	Specifies the resource group status, which can be **health**, **unhealth**, or **no_alarm_rule**. **health**: No alarms have been generated for the resource group. **unhealth**: An alarm or alarms have been generated for a resource or resources in the resource group. **no_alarm_rule**: No alarm rules have been set for the resource group.
create_time	Long	Specifies the time the resource group is created. The time is a UNIX timestamp and the unit is ms. Example: **1603819753000**
meta_data	MetaData object	Specifies the metadata of query results, including the pagination information. For details, see **Table 5-101**.
enterprise_project_id	String	Specifies the enterprise project associated with the resource group. The default value **0** indicates enterprise project **default.**

Table 5-99 resources parameter description

Parameter	Type	Description
namespace	String	Specifies the resource namespace. For example, the resource namespace of an ECS is **SYS.ECS**. To view the namespace of each service, see **Services Interconnected with Cloud Eye**.
dimensions	Arrays of objects	Specifies one or more resource dimensions. For details, see **Table 5-100**.

Parameter	Type	Description
status	String	Specifies the status of the resource group. Possible statuses are: **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.

Table 5-100 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 5-101 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.

- Response example

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



```
    "dimensions": [
      {
        "name": "instance_id",
        "value": "e37d6238-9dd3-4720-abcc-eb9f8fb08ca0"
      }
    ],
    "status": "health"
  }
],
"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 improve O&M efficiency.

URI

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

- Parameter description

  Table 5-102 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 5-103 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 5-104**.

  Table 5-104 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	Arrays of objects	Yes	Specifies one or more resource dimensions. For details, see **Table 5-105**.

Table 5-105 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 5-106 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	You are forbidden to access the page requested.
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 improve O&M efficiency.

URI

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

- Parameter description

Table 5-107 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
group_id	String	String	Specifies the resource group ID.

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

Request

- Request parameters

Table 5-108 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 5-109**.

Table 5-109 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	Arrays of objects	Yes	Specifies one or more resource dimensions. For details, see **Table 5-110**.

Table 5-110 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	You are forbidden to access the page requested.
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 5-111 Parameter description

Parameter	Type	Mandatory	Description
project_id	String	Yes	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
group_id	String	String	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 5-112 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**. **health** indicates that no alarms have been generated 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 5-113 Parameter description

Parameter	Type	Mandatory	Description
resource_groups	Array of objects	No	Specifies information about one or more resource groups. For details, see **Table 5-114**.
meta_data	MetaData object	No	Specifies the number of metadata records in the query result. For details, see **Table 5-116**.

Table 5-114 resource_groups data structure description

Parameter	Type	Mandatory	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**
instance_statistics	InstanceStatistics object	No	Specifies the resource statistics in the resource group. For details, see **Table 5-115**.
status	string	No	Specifies the status of the resource group. Possible statuses are: • **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 5-115 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.

Parameter	Type	Mandatory	Description
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 5-116 meta_data data structure description

Parameter	Type	Mandatory	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",
     "instance_statistics": {
       "unhealth": 2,
       "total": 10,
       "type_statistics": 1
     },
     "status": "unhealth",
     "enterprise_project_id": "0"
   },
   {
     "group_name": "RS",
     "create_time": 1606327955000,
     "group_id": "rg1606327955657LRj1lrE4y",
     "instance_statistics": {
       "unhealth": 0,
       "total": 2,
       "type_statistics": 1
     },
     "status": "no_alarm_rule",
     "enterprise_project_id": "0"
   },
   {
     "group_name": "RS",
     "create_time": 1606327947000,
     "group_id": "rg1606327947514v9OWqAD3N",
     "instance_statistics": {
       "unhealth": 0,
       "total": 2,
       "type_statistics": 1
     },
     "status": "no_alarm_rule",
     "enterprise_project_id": "0"
```



```
  },
  {
    "group_name": "RS",
    "create_time": 1606327946000,
    "group_id": "rg1606327946625PYogr059N",
    "instance_statistics": {
      "unhealth": 0,
      "total": 2,
      "type_statistics": 1
    },
    "status": "no_alarm_rule",
    "enterprise_project_id": "0"
  },
  {
    "group_name": "ResourceGroupCorrect_2",
    "create_time": 1606325669000,
    "group_id": "rg1606325669900Rk4eKkLMZ",
    "instance_statistics": {
      "unhealth": 0,
      "total": 1,
      "type_statistics": 1
    },
    "status": "no_alarm_rule",
    "enterprise_project_id": "0"
  }
 ],
 "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 5-117 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

- Request parameters

  Table 5-118 Parameter description

Parameter	Type	Mandatory	Description
Array elements	Arrays of objects	Yes	Specifies the event list. For details, see **Table 5-119**.

  Table 5-119 Array elements

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.

Parameter	Mandatory	Type	Description
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	Arrays of objects	Specifies the event details. For details, see **Table 5-120**.

Table 5-120 detail data structure description

Parameter	Mandatory	Type	Description
content	No	String	Specifies the event content. Enter up to 4096 characters.
group_id	No	String	Specifies the group the event belongs to. This ID must be an existing resource group ID. To query the group ID, perform the following steps: 1. Log in to the management console. 2. Click **Cloud Eye**. 3. Choose **Resource Groups**. Obtain the resource group ID in the **Name /ID** column.

Parameter	Mandatory	Type	Description
resource_id	No	String	Specifies the resource ID. Enter up to 128 characters, including letters, digits, underscores (_), hyphens (-), and colon (:). Example: 6a69bf28-ee62-49f3-9785-845dacd799ec To query the resource ID, perform the following steps: 1. Log in to the management console. 2. Under **Computing**, select **Elastic Cloud Server**. On the **Resource Overview** page, obtain the resource ID.
resource_name	No	String	Specifies the resource name. Enter up to 128 characters, including letters, digits, underscores (_), and hyphens (-).
event_state	No	String	Specifies the event status. Valid value can be **normal**, **warning**, or **incident**.
event_level	No	String	Specifies the event severity. Its value can be **Critical**, **Major**, **Minor**, or **Info**.
event_user	No	String	Specifies the event user. Enter up to 64 characters, including letters, digits, underscores (_), hyphens (-), slashes (/), and spaces.

- 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_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"
    }
}]
```

Response

- Response parameters

  Table 5-121 Parameter description

Parameter	Type	Description
Array elements	Arrays of objects	Specifies the event list. For details, see **Table 5-122**.

  Table 5-122 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":"evdgiqwgedkkcvhdjcdu346",
        "event_name":"systemInvaded"
    },
    {
        "event_id":"evdgiqwgedkkcvhdjcdu347",
        "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.

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**.

5.7.2 Querying Events

Function

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

URI

GET /V1.0/{project_id}/events

- Parameter description

Table 5-123 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**.
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.
from	Integer	No	Specifies the start time of the query. The time is a UNIX timestamp and the unit is ms. Example: **1605952700911**

Parameter	Type	Mandatory	Description
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 5-124 Parameter description

Parameter	Type	Mandatory	Description
events	Array of Events objects	No	Specifies one or more pieces of event data. For details, see **Table 5-125**.
meta_data	MetaData object	No	Specifies the number of metadata records in the query result. For details, see **Table 5-126**.

Table 5-125 events field description

Parameter	Type	Mandatory	Description
event_name	String	No	Specifies the event name.

Parameter	Type	Mandatory	Description
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	Specifies the event source. If the event is a system event, the source is the namespace of each service. To view the namespace of each service, see **Services Interconnected with Cloud Eye**. If the event is a custom event, the event source is defined by the user.

Table 5-126 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 Monitoring Details of an Event

Function

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

URI

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

- Parameter description

Table 5-127 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**.
event_name	String	Yes	Specifies the event name.

Parameter	Type	Mandatory	Description
event_type	String	Yes	Specifies the event type. Possible types are **EVENT.SYS** (system event) and **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. Possible severities are **Critical**, **Major**, **Minor**, and **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. Possible statuses are **normal**, **warning**, or **incident**.
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	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 5-128 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. Possible types are **EVENT.SYS** (system event) and **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. 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.
event_info	Array of objects	No	Specifies details about one or more events. 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 5-131**.

Table 5-129 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 5-130**.
event_id	string	No	Specifies the event ID.

Table 5-130 detail data structure description

Parameter	Type	Mandatory	Description
content	string	No	Specifies the event content. Enter up to 4096 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. Valid value can be **normal**, **warning**, or **incident**.
event_level	string	No	Specifies the event severity. Its 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. Possible types are **EVENT.SYS** (system event) and **EVENT.CUSTOM** (custom event).

Table 5-131 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"
   }
  },
  {
   "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"
   }
  },
```



```
  {
    "event_id": "ev1604654426090g7g37E6Yb",
    "event_name": "rebootServer",
    "event_source": "SYS.ECS",
    "time": 1604654425000,
    "detail": {
      "content": "{\"resourceSpecCode\":\"c6.4xlarge.2.linux\",\"enterpriseProjectId\":\"129559eb-
f795-4b5f-9e46-cbd43a462362\"}",
      "group_id": "",
      "resource_id": "0bfa63ee-31f5-40a9-b992-50992c80c58a",
      "resource_name": "ndrv2-pod-ops-0001",
      "event_state": "normal",
      "event_level": "Minor",
      "event_user": "",
      "event_type": "EVENT.SYS"
    }
  }
 ],
 "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 Permissions Policies and Supported Actions

6.1 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.

A Huawei Cloud account has all of the permissions required to call all APIs, but IAM users must have the required permissions specifically assigned. 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

6.2 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	√	×

6.3 Supported Actions of the Metric Management API

Permission	API	Action	IAM Project	Enterprise Project
Query the metric list. You can specify the namespace, metric name, dimension, sorting order, start records, and the maximum number of records when using this API to query metrics.	GET /V1.0/{project_id}/metrics	ces:metrics:list	√	×

6.4 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	√	√

6.5 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	√	×

6.6 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	√	×

6.7 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	√	×

7 Common Parameters

7.1 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.

7.2 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

```
{
    "code": 400,
    "element": "Bad Request",
    "message": "The system received a request which cannot be recognized",
    "details": {
        "details": "Some content in message body is not correct",
        "code": "ces.0014"
    }
}
```

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 correct.	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.
Kafka	500	ces.0012	The message queue is abnormal or is not ready.	The message queue is abnormal or is not ready.	Contact technical support.
Zookeeper	500	ces.0021	Internal locking error	Internal locking error	Contact technical support.

Module	HTTP Status Code	Error Code	Error Code Description	Error Message	Measure
Blueflood	500	ces.0019	The metric processing engine is abnormal.	The metric processing engine is abnormal.	Contact technical support.
Alarm	400	ces.0002	The alarm ID cannot be left blank.	The alarm ID must be specified.	Specify the alarm ID.
	403	ces.0018	The number of alarm rules created exceeds the quota.	The number of alarms exceeds the quota	Apply for a higher alarm quota.
	400	ces.0028	The metric and notification type do not match when an alarm rule is created.	The metric does not support the alarm action type.	Modify the metric or notification type according to the parameter description to make them match.

7.3 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": "65382450e8f64ac0870cd180d14e684b",
            "is_domain": false,
            "parent_id": "65382450e8f64ac0870cd180d14e684b",
            "name": "project_name",
            "description": "",
            "links": {
                "next": null,
                "previous": null,
                "self": "https://www.example.com/v3/projects/a4a5d4098fb4474fa22cd05f897d6b99"
            },
            "id": "a4a5d4098fb4474fa22cd05f897d6b99",
            "enabled": true
        }
    ],
    "links": {
        "next": null,
        "previous": null,
        "self": "https://www.example.com/v3/projects"
    }
}
```


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: AS 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
Networking	Elastic IP and bandwidth	SYS.VPC	• Key: publicip_id Value: EIP ID • Key: bandwidth_id Value: bandwidth ID
	Elastic Load Balance	SYS.ELB	• 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	• 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	• Key: direct_connect_id Value: connection • Key: history_direct_connect_id Value: historical connection

Category	Service	Namespace	Dimension
	Global Accelerator	SYS.GA	• Key: ga_accelerator_id Value: ID of the global accelerator • Key: ga_listener_id Value: ID of a listener added to the global accelerator
App middleware	Distributed Message Service	SYS.DMS	For details, see the information in the right column.
	Distributed Cache Service	SYS.DCS	• Key: dcs_instance_id Value: DCS Redis instance • Key: dcs_cluster_redis_node Value: Redis Server • Key: dcs_cluster_proxy_node Value: Proxy in a Proxy Cluster DCS Redis 3.0 instance • Key: dcs_cluster_proxy2_node Value: Proxy in a Proxy Cluster DCS of Redis 4.0 or Redis 5 instance • Key: dcs_memcached_instance_id Value: DCS Memcached instance
Database	Relational Database Service	SYS.RDS	For details, see the information in the right column.

Category	Service	Namespace	Dimension
	Document Database Service	SYS.DDS	• Key: mongodb_node_id Value: DDS node ID • Key: mongodb_instance_id Value: DDS DB instance ID
	GaussDB NoSQL	SYS.NoSQL	For details, see the information in the right column.
	GaussDB(for MySQL)	SYS.GAUSSDB	• 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

Category	Service	Namespace	Dimension
	GaussDB(for openGauss)	SYS.GAUSSDBV5	• Key: gaussdbv5_instance_id Value: GaussDB(for openGauss) instance ID • Key: gaussdbv5_node_id Value: GaussDB(for openGauss) node ID • Key: gaussdbv5_component_id Value: GaussDB(for openGauss) component ID
Enterprise Intelligence	Cloud Search Service	SYS.ES	Key: cluster_id Value: CSS cluster
	ModelArts	SYS.ModelArts	• Key: service_id Value: real-time service ID • Key: model_id Value: model ID
	Data Lake Insight	SYS.DLI	• Key: queue_id Value: queue instance • Key: flink_job_id Value: Flink job
Security	Web Application Firewall	SYS.WAF	• 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 ECS

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
ECS	Recovery started	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.
	Recovery succeeded	endAutoRecovery	Major	The ECS was recovered after the automatic migration.	This event indicates that the ECS has been recovered and been working properly.	None
	Auto recovery timeout (being processed on the backend)	faultAutoRecovery	Major	Migrating the ECS to a normal host timed out.	Migrate services to other ECSs.	Services are interrupted.
	GPU link fault	GPULinkFault	Critical	The GPU of the host running the ECS was faulty or 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.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	FPGA link fault	FPGALinkFault	Critical	The FPGA of the host running the ECS was faulty or was recovering from a fault.	Deploy service applications in HA mode. After the FPGA fault is rectified, check whether services are restored.	Services are interrupted.
	ECS or NIC exceptions occurred	vmIsRunningImproperly	Major	The ECS was faulty or the ECS NIC was abnormal.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	ECS or NIC exceptions handled	vmIsRunningImproperlyRecovery	Major	The ECS was restored to the normal status.	Wait for the ECS status to become normal and check whether services are affected.	None
	ECS deleted	deleteServer	Major	The ECS was deleted • on the management console. • by calling APIs.	Check whether the deletion was performed intentionally by a user.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ECS restarted	rebootServer	Minor	The ECS was restarted • on the management console. • by calling APIs.	Check whether the restart was performed intentionally by a user. • Deploy service applications in HA mode. • After the ECS starts up, check whether services recover.	Services are interrupted.
	ECS stopped	stopServer	Minor	The ECS was stopped • on the management console. • by calling APIs. **NOTE** The ECS is stopped only **after CTS is enabled**.	• Check whether the stop operation was performed intentionally by a user. • Deploy service applications in HA mode. • After the ECS starts up, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	NIC deleted	deleteNic	Major	The ECS NIC was deleted • on the management console. • by calling APIs.	• Check whether the deletion was performed intentionally by a user. • Deploy service applications in HA mode. • After the NIC is deleted, check whether services recover.	Services may be interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ECS resized	resizeServer	Minor	The ECS was resized • on the management console. • by calling APIs.	• Check whether the operation was performed by a user. • Deploy service applications in HA mode. • After the ECS is resized, check whether services have recovered.	Services are interrupted.
	GuestOS restarted	RestartGuestOS	Minor	The guest OS was restarted.	Contact O&M personnel.	Services may be interrupted.
	ECS failure due to abnormal host processes	VMFaultsByHostProcessExceptions	Critical	The processes of the host accommodating the ECS were abnormal.	Contact O&M personnel.	The ECS is faulty.
	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.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Live migration started	liveMigrationStarted	Major	The host where the ECS resides 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 ECS was restored to be normal after the live migration.	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.	In rare cases, services may be interrupted.
	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.

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 EIP

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
EIP	EIP bandwidth exceeded	EIPBandwidthOverflow	Major	The used bandwidth exceeded the purchased one, which may slow down the network or cause packet loss. The value of this event is the maximum value in a monitoring period, and the value of the EIP inbound and outbound bandwidth is the value at a specific time point in the period. The metrics are described as follows: **egressDropBandwidth**: dropped outbound packets (bytes) **egressAcceptBandwidth**: accepted outbound packets (bytes) **egressMaxBandwidthPerSec**: peak outbound bandwidth (bit/s) **ingressAcceptBandwidth**: accepted inbound packets (bytes) **ingressMaxBandwidthPerSec**:	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	Event Name	Event ID	Event Severity	Description	Solution	Impact
				peak inbound bandwidth (bit/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
	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.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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	Event Name	Event ID	Event Severity	Description	Solution	Impact
	QoS bandwidth exceeded	EIPBandwidthRuleOverflow	Major	The used QoS bandwidth exceeded the allocated one, which may slow down the network or cause packet loss. The value of this event is the maximum value in a monitoring period, and the value of the EIP inbound and outbound bandwidth is the value at a specific time point in the period. **egressDropBandwidth**: dropped outbound packets (bytes) **egressAcceptBandwidth**: accepted outbound packets (bytes) **egressMaxBandwidthPerSec**: peak outbound bandwidth (bit/s) **ingressAcceptBandwidth**: accepted inbound packets (bytes) **ingressMaxBandwidthPerSec**: peak inbound bandwidth (bit/s)	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	Event Name	Event ID	Event Severity	Description	Solution	Impact
				ingressDropBandwidth: dropped inbound packets (bytes)		

Table A-3 Advanced Anti-DDoS (AAD)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
AAD	DDoS Attack Events	ddosAttackEvents	Major	A DDoS attack occurs in the AAD protected lines.	Judge the impact on services based on the attack traffic and attack type. If the attack traffic exceeds your purchased elastic bandwidth, change to another line or increase your bandwidth.	Services may be interrupted.

Table A-4 CBR

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
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.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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
	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

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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-5 RDS — operations

Event Source	Event Name	Event ID	Event Severity
RDS	Reset administrator password	resetPassword	Major
	Operate DB instance	instanceAction	Major
	Delete DB instance	deleteInstance	Minor
	Modify backup policy	setBackupPolicy	Minor
	Change parameter group	updateParameterGroup	Minor
	Delete parameter group	deleteParameterGroup	Minor
	Reset parameter group	resetParameterGroup	Minor

Event Source	Event Name	Event ID	Event Severity
	Change database port	changeInstancePort	Major
	Primary/standby switchover or failover	PrimaryStandbySwitched	Major

Table A-6 DDS

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
DDS	DB instance creation failure	DDSCreateInstanceFailed	Major	A DDS instance fails to be created due to insufficient disks, quotas, and underlying resources.	Check the number and quota of disks. Release resources and create DDS instances again.	DDS instances cannot be created.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Replication failed	DDSAbnormalReplicationStatus	Major	The possible causes are as follows: • The replication delay between the primary and standby instances is too long, which usually occurs when a large amount of data is written to databases or a large transaction is performed. During off-peak hours, the replication delay gradually decreases. • The network between the primary and standby instances is disconnected.	Submit a service ticket.	Your applications are not affected because this event does not interrupt data read and write.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Replication recovered	DDSReplicationStatusRecovered	Major	The replication delay between the primary and standby instances is within the normal range, or the network connection between them has restored.	No action is required.	None
	DB instance failed	DDSFaultyDBInstance	Major	This event is a key alarm event and is reported when an instance was faulty due to a disaster or a server failure.	Submit a service ticket.	The database service may be unavailable.
	DB instance recovered	DDSDBInstanceRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None
	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.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Node recovered	DDSDBNodeRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None
	Primary/standby switchover or failover	DDSPrimaryStandbySwitched	Major	A primary/standby switchover is performed or a failover is triggered.	No action is required.	None
	Insufficient data disk space	DDSRiskyDataDiskUsage	Major	The data disk space is insufficient.	Expand the disk capacity. For details, see section "Scaling Up Storage Space" in the user guide of the corresponding service.	The instance is set to read-only and data cannot be written to the instance.
	Data disk expanded and restored to writable	DDSDataDiskUsageRecovered	Major	The data disk capacity has been expanded and the data disk becomes writable.	No action is required.	None

Table A-7 GaussDB NoSQL

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
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.
	Specifications modification failed	NoSQLResizeInstanceFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you need to change the specifications again.	Services are interrupted.
	Node adding failed	NoSQLAddNodesFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you delete the node that failed to be added and add a new node.	None
	Node deletion failed	NoSQLDeleteNodesFailed	Major	The underlying resources fail to be released.	Delete the node again.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Storage space scale-up failed	NoSQLScaleUpStorageFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background and then you scale up the storage space again.	Services may be interrupted.
	Password reset failed	NoSQLResetPasswordFailed	Major	Resetting the password times out.	Reset the password again.	None
	Parameter group change failed	NoSQLUpdateInstanceParamGroupFailed	Major	Changing a parameter group times out.	Change the parameter group again.	None
	Backup policy configuration failed	NoSQLSetBackupPolicyFailed	Major	The database connection is abnormal.	Configure the backup policy again.	None
	Manual backup creation failed	NoSQLCreateManualBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
	Automated backup creation failed	NoSQLCreateAutomatedBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Faulty DB instance	NoSQLFaultyDBInstance	Major	This event was a key alarm event and is reported when an instance was faulty due to a disaster or a server failure.	Submit a service ticket.	The database service may be unavailable.
	DB instance recovered	NoSQLDBInstanceRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None
	Faulty node	NoSQLFaultyDBNode	Major	This event is a key alarm event and is reported when a database node is faulty due to a disaster or a server failure.	Check whether the database service is available and submit a service ticket.	The database service may be unavailable.
	Node recovered	NoSQLDBNodeRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Primary/standby switchover or failover	NoSQLPrimaryStandbySwitched	Major	This event is reported when a primary/standby switchover is performed or a failover is triggered.	No action is required.	None
	HotKey occurred	HotKeyOccurs	Major	The primary key is improperly configured. As a result, hotspot data is distributed in one partition. The improper application design causes frequent read and write operations on a key.	1. Choose a proper partition key. 2. Add service cache. The service application reads hotspot data from the cache first.	The service request success rate is affected, and the cluster performance and stability also be affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	BigKey occurred	BigKeyOccurs	Major	The primary key design is improper. The number of records or data in a single partition is too large, causing unbalanced node loads.	1. Choose a proper partition key. 2. Add a new partition key for hashing data.	As the data in the large partition increases, the cluster stability deteriorates.
	Insufficient storage space	NoSQLRiskyDataDiskUsage	Major	The storage space is insufficient.	Scale up storage space. For details, see section "Scaling Up Storage Space" in the corresponding user guide.	The instance is set to read-only and data cannot be written to the instance.
	Data disk expanded and being writable	NoSQLDataDiskUsageRecovered	Major	The capacity of a data disk has been expanded and the data disk becomes writable.	No operation is required.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Index creation failed	NoSQLCreateIndexFailed	Major	The service load exceeds what the instance specifications can take. In this case, creating indexes consumes more instance resources. As a result, the response is slow or even frame freezing occurs, and the creation times out.	Select the matched instance specifications based on the service load. Create indexes during off-peak hours. Create indexes in the background. Select indexes as required.	The index fails to be created or is incomplete. As a result, the index is invalid. Delete the index and create an index.
	Write speed decreased	NoSQLStallingOccurs	Major	The write speed is fast, which is close to the maximum write capability allowed by the cluster scale and instance specifications. As a result, the flow control mechanism of the database is triggered, and requests may fail.	1. Adjust the cluster scale or node specifications based on the maximum write rate of services. 2. Measures the maximum write rate of services.	The success rate of service requests is affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Data write stopped	NoSQLStoppingOccurs	Major	The data write is too fast, reaching the maximum write capability allowed by the cluster scale and instance specifications. As a result, the flow control mechanism of the database is triggered, and requests may fail.	1. Adjust the cluster scale or node specifications based on the maximum write rate of services. 2. Measures the maximum write rate of services.	The success rate of service requests is affected.
	Database restart failed	NoSQLRestartDBFailed	Major	The instance status is abnormal.	Submit a service ticket to the O&M personnel.	The DB instance status may be abnormal.
	Restoration to new DB instance failed	NoSQLRestoreToNewInstanceFailed	Major	The underlying resources are insufficient.	Submit a service order to ask the O&M personnel to coordinate resources in the background and add new nodes.	Data cannot be restored to a new DB instance.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Restoration to existing DB instance failed	NoSQLRestoreToExistInstanceFailed	Major	The backup file fails to be downloaded or restored.	Submit a service ticket to the O&M personnel.	The current DB instance may be unavailable.
	Backup file deletion failed	NoSQLDeleteBackupFailed	Major	The backup files fail to be deleted from OBS.	Delete the backup files again.	None
	Failed to enable Show Original Log	NoSQLSwitchSlowlogPlainTextFailed	Major	The DB engine does not support this function.	Refer to the *GaussDB NoSQL User Guide* to ensure that the DB engine supports Show Original Log. Submit a service ticket to the O&M personnel.	None
	EIP binding failed	NoSQLBindEipFailed	Major	The node status is abnormal, an EIP has been bound to the node, or the EIP to be bound is invalid.	Check whether the node is normal and whether the EIP is valid.	The DB instance cannot be accessed from the Internet.
	EIP unbinding failed	NoSQLUnbindEipFailed	Major	The node status is abnormal or the EIP has been unbound from the node.	Check whether the node and EIP status are normal.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Parameter modification failed	NoSQLModifyParameterFailed	Major	The parameter value is invalid.	Check whether the parameter value is within the valid range and submit a service ticket to the O&M personnel.	None
	Parameter group application failed	NoSQLApplyParameterGroupFailed	Major	The instance status is abnormal. As a result, the parameter group cannot be applied.	Submit a service ticket to the O&M personnel.	None
	Failed to enable or disable SSL	NoSQLSwitchSSLFailed	Major	Enabling or disabling SSL times out.	Try again or submit a service ticket. Do not change the connection mode.	The connection mode cannot be changed.

Table A-8 GaussDB(for MySQL)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB(for MySQL)	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	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	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Read replica deletion failure	TaurusDeleteReadOnlyNodeFailed	Major	The communications between the management plane and the read replica are abnormal or the VM fails to be deleted from IaaS.	Submit a service ticket.	Read replicas fail to be deleted.
	Password reset failure	TaurusResetInstancePasswordFailed	Major	The communications between the management plane and the instance are abnormal or the instance is abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Passwords fail to be reset for instances.
	DB instance reboot failure	TaurusRestartInstanceFailed	Major	The network between the management plane and the instance is abnormal or the instance is abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Instances fail to be rebooted.
	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.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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.
	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	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Primary/standby failover	TaurusActiveStandbySwitched	Major	When the network, physical machine, or database of the primary node is faulty, the system promotes a read replica to primary based on the failover priority to ensure service continuity.	1. Check whether the service is running properly. 2. Check whether an alarm is generated, indicating that the read replica failed to be promoted to primary.	During the failover, database connection is interrupted for a short period of time. After the failover is complete, you can reconnect to the database.
	数据库设置为只读模式	NodeReadonlyMode	重要	数据库设置为只读状态，只支持查询类操作。	联系数据库技术支持团队处理。	数据库设置只读状态后，所有写业务返回失败。
	数据库设置为读写模式	NodeReadWriteMode	重要	数据库设置为读写状态	无	无

Table A-9 GaussDB(for openGauss)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB(for openGauss)	Process status alarm	ProcessStatusAlarm	Major	Key processes exit, including: CMS/CMA, ETCD, GTM, CN, or DN process.	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, or DN component.	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	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	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Other abnormal alarm	OtherAbnormalAlarm	Major	Disk usage threshold alarm	Focus on service changes and scale up storage space as needed.	If the used storage space exceeds the threshold, storage space cannot be scaled up.
	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(for 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	Event Name	Event ID	Event Severity	Description	Solution	Impact
	DB node recovered	TaurusNodeRunningStatusRecovered	Major	GaussDB(for 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.
	Node adding failure	GaussDBV5ExpandClusterFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you delete the node that failed to be added and add a new node.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Storage scale-up failure	GaussDBV5EnlargeVolumeFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background and then you scale up the storage space again.	Services may be interrupted.
	Reboot failure	GaussDBV5RestartInstanceFailed	Major	The network is abnormal.	Retry the reboot operation or submit a service ticket to the O&M personnel.	The database service may be unavailable.
	Full backup failure	GaussDBV5FullBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
	Differential backup failure	GaussDBV5DifferentialBackupFailed	Major	The backup files fail to be exported or uploaded.	Submit a service ticket to the O&M personnel.	Data cannot be backed up.
	Backup deletion failure	GaussDBV5DeleteBackupFailed	Major	This function does not need to be implemented.	N/A	N/A

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	EIP binding failure	GaussDBV5BindEIPFailed	Major	The EIP is bound to another resource.	Submit a service ticket to the O&M personnel.	The instance cannot be accessed from the Internet.
	EIP unbinding failure	GaussDBV5UnbindEIPFailed	Major	The network is faulty or EIP is abnormal.	Unbind the IP address again or submit a service ticket to the O&M personnel.	IP addresses may be residual.
	Parameter template application failure	GaussDBV5ApplyParamFailed	Major	Modifying a parameter template times out.	Modify the parameter template again.	None
	Parameter modification failure	GaussDBV5UpdateInstanceParamGroupFailed	Major	Modifying a parameter template times out.	Modify the parameter template again.	None
	Backup and restoration failure	GaussDBV5RestoreFromBcakupFailed	Major	The underlying resources are insufficient or backup files fail to be downloaded.	Submit a service ticket.	The database service may be unavailable during the restoration failure.

Table A-10 DDM

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
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.
	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	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Failed to create a schema	createLogicDbFailed	Major	The possible causes are as follows: • The DB instance account is incorrect. • The DDM instance and its associated DB instances cannot communicate with each other because their security groups are not configured correctly.	Check the following items: • Whether the DB instance account is correct. • Whether the security groups associated with the DDM instance and its associated DB instance are correctly configured.	Services cannot run properly.
	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-11 Cloud Phone

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
CPH	Server shutdown	cphServerOsShutdown	Major	The cloud phone server was shut down • on the management console. • by calling APIs.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	Server abnormal shutdown	cphServerShutdown	Major	The cloud phone server was shut down unexpectedly. Possible causes are as follows: • The cloud phone server was powered off unexpectedly. • The cloud phone server was shut down due to hardware faults.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	Server reboot	cphServerOsReboot	Major	The cloud phone server was rebooted • on the management console. • by calling APIs.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Server abnormal reboot	cphServerReboot	Major	The cloud phone server was rebooted unexpectedly. Possible causes are as follows: • OS faults • Hardware faults	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	Network disconnection	cphServerlinkDown	Major	The network where the cloud phone server was deployed was disconnected. Possible causes are as follows: • The cloud phone server was shut down unexpectedly and rebooted. • The switch was faulty. • The gateway node was faulty.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Services are interrupted.
	PCIe error	cphServerPcieError	Major	The PCIe device or main board on the cloud phone server was faulty. Possible causes are as follows: • Mainboard faults • PCIe device faults	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	The network or disk read/ write is affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Disk error	cphServerDiskError	Major	The disk on the cloud phone server was faulty. Possible causes are as follows: • Disk backplane faults • Disk faults	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Data read/ write services are affected, or the BMS cannot be started.
	Storage error	cphServerStorageError	Major	The cloud phone server could not connect to EVS disks. Possible causes are as follows: • SDI card faults • Remote storage devices were faulty.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Data read/ write services are affected, or the BMS cannot be started.
	GPU offline	cphServerGpuOffline	Major	GPU of the cloud phone server was loose and disconnected.	Stop the cloud phone server and reboot it.	Faults occur on cloud phones whose GPUs are disconnected. Cloud phones cannot run properly even if they are restarted or reconfigured.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	GPU timeout	cphServerGpuTimeOut	Major	GPU of the cloud phone server timed out.	Reboot the cloud phone server.	Cloud phones whose GPUs timed out cannot run properly and are still faulty even if they are restarted or reconfigured.
	Disk space full	cphServerDiskFull	Major	Disk space of the cloud phone server was used up.	Clear the application data in the cloud phone to release space.	Cloud phone is sub-healthy, prone to failure, and unable to start.
	Disk readonly	cphServerDiskReadOnly	Major	The disk of the cloud phone server became read-only.	Reboot the cloud phone server.	Cloud phone is sub-healthy, prone to failure, and unable to start.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Cloud phone metadata damaged	cphPhoneMetaDataDamage	Major	Cloud phone metadata was damaged.	Contact Huawei O&M personnel.	The cloud phone cannot run properly even if it is restarted or reconfigured.

Table A-12 L2CG

EventSource	Event Name	Event ID	Event Severity	Description	Solution	Impact
L2CG	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-13 VPC

Event Source	Event Name	Event ID	Event Severity
VPC	VPC deleted	deleteVpc	Major
	VPC modified	modifyVpc	Minor
	Subnet deleted	deleteSubnet	Minor
	Subnet modified	modifySubnet	Minor

Event Source	Event Name	Event ID	Event Severity
	Bandwidth modified	modifyBandwidth	Minor
	VPN deleted	deleteVpn	Major
	VPN modified	modifyVpn	Minor

Table A-14 EVS

Event Source	Event Name	Event ID	Event Severity
EVS	Disk updated	updateVolume	Minor
	Disk expanded	extendVolume	Minor
	Disk deleted	deleteVolume	Major

Table A-15 IAM

Event Source	Event Name	Event ID	Event Severity
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

Event Source	Event Name	Event ID	Event Severity
	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-16 KMS

Event Source	Event Name	Event ID	Event Severity
KMS	Key disabled	disableKey	Major
	Key deletion scheduled	scheduleKeyDeletion	Minor
	Grant retired	retireGrant	Major
	Grant revoked	revokeGrant	Major

Table A-17 OBS

Event Source	Event Name	Event ID	Event Severity
OBS	Bucket deleted	deleteBucket	Major
	Bucket policy deleted	deleteBucketPolicy	Major
	Bucket ACL configured	setBucketAcl	Minor
	Bucket policy configured	setBucketPolicy	Minor

Table A-18 DCS

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
DCS	Full synchronization during online migration retry	migrationFullResync	Minor	If online migration fails, full synchronization will be triggered because incremental synchronization cannot be performed.	Monitor the service volume and bandwidth usage. If the bandwidth usage is high and affects the service, manually stop the migration as required.	If the data volume is large, full synchronization may cause bandwidth usage to spike.
	Redis master/ replica switchover	masterStandbyFailover	Minor	The master node was abnormal, promoting a replica to master.	Check the original master node and rectify the fault.	None
	Memcached master/ standby switchover	memcachedMasterStandbyFailover	Minor	The master node was abnormal, promoting the standby node to master.	Check the original master node and rectify the fault.	None
	Redis server exception	redisNodeStatusAbnormal	Major	The Redis server status was abnormal.	Check the Redis server status.	The instance may become unavailable.
	Redis server recovered	redisNodeStatusNormal	Major	The Redis server status recovered.	None	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Synchronization failure in data migration	migrateSyncDataFail	Major	Online migration failed.	Check the network and the ECS service. If the ECS service is abnormal, a migration ECS cannot be created.	Data cannot be synchronized.
	Memcached instance abnormal	memcachedInstanceStatusAbnormal	Major	The Memcached node status was abnormal.	Check the Memcached node status.	The instance may become unavailable.
	Memcached instance recovered	memcachedInstanceStatusNormal	Major	The Memcached node status recovered.	None	None
	Instance backup failure	instanceBackupFailure	Major	The DCS instance fails to be backed up due to an OBS access failure.	Manually back up the instance again.	None
	Instance node abnormal restart	instanceNodeAbnormalRestart	Major	DCS nodes restarted unexpectedly when they became faulty.	Check whether services are normal.	Master/standby switchover may occur or access to Redis may fail.

B Change History

Released On	Description
2022-09-30	This issue is the first official release.

