Cloud Eye

API Reference

Issue 02

Date 2022-12-31

HUAWEI

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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

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?" in the *Cloud Eye User Guide*.

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**.

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**.

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" in the *Cloud Eye User Guide*.
- 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

  A region is a geographic area in which cloud resources are deployed. Availability zones (AZs) in the same region can communicate with each other over an intranet, while AZs in different regions are isolated from each other. Deploying cloud resources in different regions can better suit certain user requirements or comply with local laws or regulations.

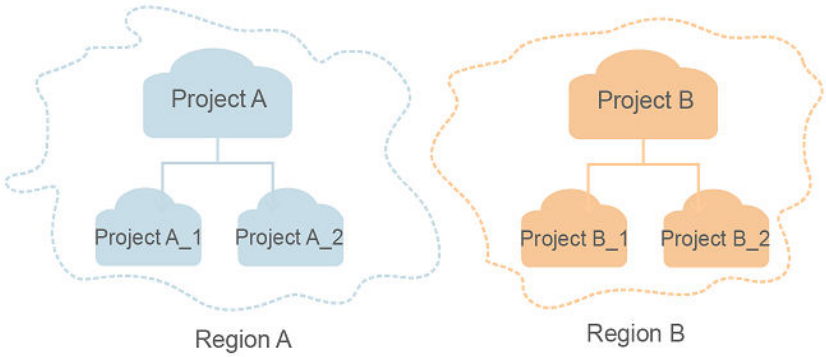
- AZ

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

- Project

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

Figure 1-1 Project isolation model



2 API Overview

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

Table 2-1 API description

Type	Subtype	API	Description
API V1	API version management	Querying All API Versions	Query all API versions supported by Cloud Eye.
		Querying a Specified API Version	Query a specified API version supported by Cloud Eye.
	Metric management	Querying Metrics	Query the list of metrics that currently monitored by Cloud Eye.
	Alarm rule management	Querying Alarm Rules	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.
		Querying the Host Configuration	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.
	Quota management	Querying Quotas	Query the alarm rule quota.
	Event monitoring	Reporting Events	Report custom events.
API V2	Alarm rule	Creating an Alarm Rule	Create an alarm rule.
		Deleting Alarm Rules in Batches	Delete alarm rules in batches.
		Enabling or Disabling Alarm Rules in Batches	Enable or disable alarm rules in batches.
		Querying Alarm Rules	Query alarm rules.
		Adding Alarm Rules in Batches	Add alarm rules in batches. (Alarm rules for resources in resource groups are not excluded.)
		Deleting Alarm Rules in Batches	Delete alarm rules in batches. (Alarm rules for resources in resource groups are excluded.)
		Querying Alarm Rules	Query cloud service resources configured in an alarm rule based on the alarm rule ID.
		Modify Policies in an Alarm Rule	Modify policies in an alarm rule.
		Querying Alarm Policies	Query alarm policies based on the alarm rule ID.
	Alarm records	Querying Alarm Records.	Query alarm records.

Type	Subtype	API	Description
	Metric management	Querying Server Monitoring Metrics	Query metrics by disk, mount point, process, graphics card, or RAID controller based on the ECS or BMS ID.

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

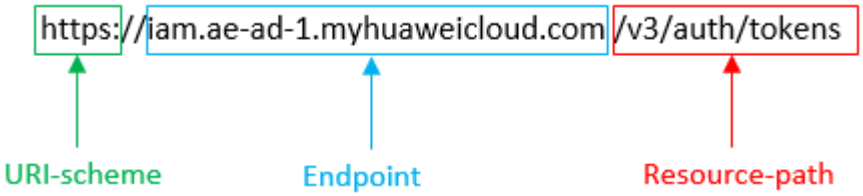
Parameter	Description
URI-scheme	Protocol used to transmit requests. All APIs use HTTPS.
Endpoint	Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from **Regions and Endpoints**. For example, the endpoint of IAM in the **UAE-Abu Dhabi** region is **iam.ae-ad-1.myhuaweicloud.com**.
resource-path	Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.

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 **UAE-Abu Dhabi** region, obtain the endpoint of IAM (**iam.ae-ad-1.myhuaweicloud.com**) 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.ae-ad-1.myhuaweicloud.com/v3/auth/tokens
```

Figure 3-1 Example URI



NOTE

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

Request Methods

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

Table 3-2 HTTP methods

Method	Description
GET	Requests the server to return specified resources.
PUT	Requests the server to update specified resources.
POST	Requests the server to add resources or perform special operations.
DELETE	Requests the server to delete specified resources, for example, an object.
HEAD	Same as GET except that the server must return only the response header.

Method	Description
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.ae-ad-1.myhuaweicloud.com/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

Parameter	Description	Mandatory	Example Value
X-Project-Id	Specifies the project ID. Obtain the project ID by following the instructions in **Obtaining a Project ID**.	No	e9993fc787d94b6c886cbaa340f9c0f4
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.ae-ad-1.myhuaweicloud.com/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.ae-ad-1.myhuaweicloud.com/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.

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

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

```
POST https://iam.ae-ad-1.myhuaweicloud.com/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 3-2 shows the response header fields for the API used to **obtain a user token**. The **x-subject-token** header field is the desired user token. This token can then be used to authenticate the calling of other APIs.

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

(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 API DescriptionAPI V1

4.1 API Version Management

4.1.1 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 4-1 Parameter description

Parameter	Type	Description
versions	Array of objects	Specifies the list of all versions. For details, see **Table 4-2**.

Table 4-2 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 4-3**.
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 4-3 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**.

4.1.2 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 4-4 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 4-5 Parameter description

Parameter	Type	Description
version	Objects	Specifies the list of all versions. For details, see **Table 4-6**.

Table 4-6 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 4-7**.
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 4-7 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**.

4.2 Metric Management

4.2.1 Querying 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 4-8 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 4-9 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 4-10 Parameter description

Parameter	Type	Description
metrics	Array of objects	Specifies the list of metric objects. For details, see **Table 4-11**.
meta_data	Object	Specifies the metadata of query results, including the pagination information. For details, see **Table 4-13**.

Table 4-11 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 4-12**.
metric_name	String	Specifies the metric name, such as **cpu_util**.
unit	String	Specifies the metric unit.

Table 4-12 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 4-13 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**.

4.3 Alarm Rule Management

4.3.1 Querying Alarm Rules

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 4-14 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 4-15 Parameter description

Parameter	Type	Description
alarms	Array of objects	Specifies the alarm rule list. For details, see **Table 4-16**.

Table 4-16 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 4-17 Response parameters

Parameter	Type	Description
metric_alarms	Array of objects	Specifies the list of alarm objects. For details, see **Table 4-18**.
meta_data	Object	Specifies the metadata of query results, including the pagination information. For details, see **Table 4-24**.

Table 4-18 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 4-19**.
condition	Object	Specifies the alarm triggering condition. For details, see **Table 4-23**.
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 4-21**.
ok_actions	Array of objects	Specifies the action to be triggered after the alarm is cleared. For details, see **Table 4-22**.
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 4-19 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 4-20**.
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**.

Table 4-20 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 4-21 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.

Parameter	Type	Description
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 4-22 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 4-23 condition data structure description

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

Parameter	Type	Description
value	Double	Specifies the alarm threshold. Supported range: **0** to **Number. MAX_VALUE (1.7976931348623157e+108)** For detailed thresholds, see the value range of each metric in the appendix. For example, you can set 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**

Table 4-24 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**.

4.3.2 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 4-25 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**.
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 4-26**.

Table 4-26 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 4-27**.
condition	Object	Specifies the alarm triggering condition. For details, see **Table 4-31**.
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 4-29**.
ok_actions	Array of objects	Specifies the action to be triggered after the alarm is cleared. For details, see **Table 4-30**.
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 4-27 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 4-28**.
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**.

Table 4-28 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 4-29 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 4-30 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 4-31 condition data structure description

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

Parameter	Type	Description
count	Integer	Specifies the number of consecutive occurrence times that the alarm policy was met. Supported range: **1** to **5**

- 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**.

4.3.3 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 4-32 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 4-33 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.
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**.

4.3.4 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 4-34 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.

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**.

4.3.5 Creating an Alarm Rule

Function

This API is used to create an alarm rule.

URI

POST /V1.0/{project_id}/alarms

- Parameter description

  Table 4-35 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 4-36 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.

Parameter	Mandatory	Type	Description
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 4-37**.
condition	Yes	Object	Specifies the alarm triggering condition. For details, see **Table 4-41**.
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**.)
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.

Parameter	Mandatory	Type	Description

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 4-39**.

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 4-40**.

Table 4-37 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 4-38**.

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

Table 4-38 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. Start with a letter or a digit. Enter 1 to 256 characters. Only letters, digits, underscores (_), and hyphens (-) are allowed.

Table 4-39 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.
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 4-40 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 4-41 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.

Parameter	Mandatory	Type	Description
count	Yes	Integer	Specifies the number of consecutive occurrence times that the alarm policy was met. Supported range: **1** to **5**

- 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"]
      }
   ]
}
```

Response

- Response parameters

Table 4-42 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**.

4.4 Monitoring Data Management

4.4.1 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 4-43 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 4-44 Query parameter description

Parameter	Mandatory	Type	Description
namespace	Yes	String	Specifies the namespace of a service. For details, see **Services Interconnected with Cloud Eye**. The namespace must be in the **service.item** format and contain 3 to 32 characters. **service** and **item** each must start with a letter and contain only letters, digits, and underscores (_).
metric_name	Yes	String	Specifies the metric name. You can obtain the metric names of existing alarm rules by referring to **Querying Metrics**.
from	Yes	String	Specifies the start time of the query. The time is a UNIX timestamp and the unit is ms. Rollup aggregates the raw data generated within a period to the start time of the period. 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.

Parameter	Mandatory	Type	Description
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**.
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 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 4-45 Response parameters

Parameter	Type	Description
datapoints	Array of objects	Specifies the metric data list. For details, see **Table 4-46**. 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 4-46 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**.

4.4.2 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 4-47 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 4-48 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 4-49**.

Table 4-49 Array elements

Parameter	Mandatory	Type	Description
metric	Yes	Object	Specifies the metric data. For details, see **Table 4-50**.
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 4-50 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**, **AGT**, or **SRE**, 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 4-51**.
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 4-51 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 a custom dimension. The instance ID is **6f3c6f91-4b24-4e1b-b7d1-a94ac1cb011d**.

```
[
  {
    "metric": {
      "namespace": "MINE.APP",
      "dimensions": [
        {
          "name": "instance_id",
          "value": "6f3c6f91-4b24-4e1b-b7d1-a94ac1cb011d"
        }
      ],
      "metric_name": "cpu_util"
    },
    "ttl": 172800,
    "collect_time": 1463598260000,
    "type": "float",
    "value": 0.09,
    "unit": "%"
  },
  {
    "metric": {
      "namespace": "MINE.APP",
      "dimensions": [
        {
          "name": "instance_id",
          "value": "6f3c6f91-4b24-4e1b-b7d1-a94ac1cb011d"
        }
      ],
      "metric_name": "cpu_util"
    },
    "ttl": 172800,
    "collect_time": 1463598270000,
    "type": "float",
    "value": 0.12,
    "unit": "%"
  }
]
```

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

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



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

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

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

Response

The response has no message body.

Returned Values

- Normal

  201

- Abnormal

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

4.4.3 Querying the Host Configuration

Function

This API is used to 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.

NOTICE

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

URI

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

- Parameter description

  Table 4-52 Parameter description

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

- Parameters that are used to query the host configuration

Parameter	Mandatory	Type	Description
namespace	Yes	String	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 (_).
type	Yes	String	Specifies the event type. It can contain only letters, underscores (_), and hyphens (-). It must start with a letter and cannot exceed 64 characters, for example, **instance_host_info**.
from	Yes	String	Specifies the start time of the query. The time is a UNIX timestamp and the unit is ms.
to	Yes	String	Specifies the end time of the query. The time is a UNIX timestamp and the unit is ms. **from** must be earlier than **to**.
dim	Yes	String	Specifies the dimension. For example, the ECS dimension is **instance_id**. For details about the dimensions corresponding to the monitoring metrics of each service, see the monitoring metrics description of the corresponding service in **Services Interconnected with Cloud Eye**. Specifies the dimension. A maximum of three dimensions are supported, and the dimensions are numbered from 0 in **dim.{i}=key,value** format. **key** cannot exceed 32 characters and **value** cannot exceed 256 characters. Example: **dim.0=instance_id,i-12345**

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

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

Request

None

Response

- Response parameters

Table 4-53 Response parameters

Parameter	Type	Description
datapoints	Array of objects	Specifies the configuration list. If the corresponding configuration information does not exist, **datapoints** is an empty array and is **[]**. For details, see **Table 4-54**.

Table 4-54 datapoints data structure description

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

- Example response

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

Returned Values

- Normal

  200
- Abnormal

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

4.5 Quota Management

4.5.1 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 4-55 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 4-56 Response parameters

Parameter	Type	Description
quotas	Object	Specifies the quota list. For details, see **Table 4-57**.

Table 4-57 Data structure description of **quotas**

Parameter	Type	Description
resources	Array of objects	Specifies the resource quota list. For details, see **Table 4-58**.

Table 4-58 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**.

4.6 Event Monitoring

4.6.1 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 4-59 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 4-60 Parameter description

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

  Table 4-61 Parameter description of the **EventItem** field

Parameter	Mandatory	Type	Description
event_name	Yes	String	Specifies the event name. Start with a letter. Enter 1 to 64 characters. Only letters, digits, and underscores (_) are allowed.
event_source	Yes	String	Specifies the event source. The format is service.item. Set this parameter based on the site requirements. **service** and **item** each must be a string that starts with a letter and contains 3 to 32 characters, including only letters, digits, and underscores (_).

Parameter	Mandatory	Type	Description
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	Details of objects	Specifies the event details. For details, see **Table 4-62**.

Table 4-62 detail data structure description

Parameter	Mandatory	Type	Description
content	No	String	Specifies the event content. Enter up to 4096 characters.
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**.

Parameter	Mandatory	Type	Description
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.
event_type	No	String	Specifies the event type. Its value can be **EVENT.SYS** or **EVENT.CUSTOM**. **EVENT.SYS** indicates system events that cannot be reported by users. Only custom events can be reported.

- Example request

```
[{
   "event_name":"systemInvaded",
   "event_source":"financial.System",
   "time":1522121194000,
   "detail":{
      "content":"The financial system was invaded",
      "group_id":"rg15221211517051YWWkEnVd",
      "resource_id":"1234567890sjgggad",
      "resource_name":"ecs001",
      "event_state":"normal",
      "event_level":"Major",
      "event_user":"xiaokong",
      "event_type": "EVENT.CUSTOM"
   }
},
{
   "event_name":"systemInvaded",
   "event_source":"financial.System",
   "time":1522121194020,
   "detail":{
      "content":"The financial system was invaded",
      "group_id":"rg15221211517051YWWkEnVd",
      "resource_id":"1234567890sjgggad",
      "resource_name":"ecs001",
      "event_state":"normal",
      "event_level":"Major",
      "event_user":"xihong",
      "event_type": "EVENT.CUSTOM"
   }
}]
```

Response

- Response parameters

Table 4-63 Parameter description

Parameter	Type	Description
Array elements	Arrays of objects	Specifies the event list. For details, see **Table 4-64**.

Table 4-64 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.
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 API v2

5.1 Alarm Resources

5.1.1 Adding Alarm Rules in Batches

Function

This API is used to add alarm rules in batches (alarm rules configured in resource groups are not supported). To manage resource groups, use related resource group management interfaces.

URI

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

Table 5-1 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: **1** Maximum: **64** **Regex Pattern:** ^[a-zA-Z0-9-]{1,64}$
alarm_id	Yes	String	Specifies the ID of the instance for which the alarm rule is configured. **Regex Pattern:** al([a-z]|[A-Z]|[0-9]){22}$

Request Parameters

Table 5-2 Request header parameters

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

Table 5-3 Request body parameters

Parameter	Mandatory	Type	Description
resources	Yes	Array<Array< **Dimension**>>	Specifies the resource information.

Table 5-4 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Resource dimension. For example, the dimension of an ECS is instance_id. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){1,32}$

Parameter	Mandatory	Type	Description
value	No	String	Specifies the value of a resource dimension, which is the resource instance ID, for example, 4270ff17-aba3-4138-89fa-820594c39755. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]){1}([a-z]|[A-Z]|[0-9]|_|-|\.)*)|*){1,256}$

Response Parameters

Status code: 400

Table 5-5 Response body parameters

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

Status code: 404

Table 5-6 Response body parameters

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

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

Status code: 500

Table 5-7 Response body parameters

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

Example Requests

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

Example Responses

None

Status Codes

Status Code	Description
200	Alarm rules added.

Status Code	Description
400	Parameter verification failed.
404	Alarm rules not found.
500	System error.

Error Codes

See **Error Codes**.

5.1.2 Deleting Alarm Rules in Batches

Function

This API is used to delete alarm rules in batches (alarm rules configured in resource groups are not supported). To modify the alarm rules configured in resource groups, use the resource group management interfaces.

URI

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

Table 5-8 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: **1** Maximum: **64** **Regex Pattern:** ^[a-zA-Z0-9-]{1,64}$
alarm_id	Yes	String	Specifies the ID of the instance for which the alarm rule is configured. **Regex Pattern:** al([a-z]|[A-Z]|[0-9]){22}$

Request Parameters

Table 5-9 Request header parameters

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

Table 5-10 Request body parameters

Parameter	Mandatory	Type	Description
resources	Yes	Array<Array< **Dimension**>>	Specifies the resource information.

Table 5-11 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Resource dimension. For example, the dimension of an ECS is instance_id. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){1,32}$

Parameter	Mandatory	Type	Description
value	No	String	Specifies the value of a resource dimension, which is the resource instance ID, for example, 4270ff17-aba3-4138-89fa-820594c39755. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]){1}([a-z]|[A-Z]|[0-9]|_|-|\.)*)|*){1,256}$

Response Parameters

Status code: 400

Table 5-12 Response body parameters

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

Status code: 404

Table 5-13 Response body parameters

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

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

Status code: 500

Table 5-14 Response body parameters

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

Example Requests

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

Example Responses

None

Status Codes

Status Code	Description
200	Alarm rules deleted.

Status Code	Description
400	Parameter verification failed.
404	Alarm rules not found.
500	System error.

Error Codes

See **Error Codes**.

5.1.3 Querying Alarm Rules

Function

This API is used to query alarm rules based on the alarm rule ID.

URI

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

Table 5-15 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: **1** Maximum: **64** **Regex Pattern:** ^[a-zA-Z0-9-]{1,64}$
alarm_id	Yes	String	Specifies the ID of the instance for which an alarm rule is configured. **Regex Pattern:** al([a-z]|[A-Z]|[0-9]){22}$

Table 5-16 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Specifies the pagination offset. Minimum: **0** Maximum: **10000** Default: **0** **Regex Pattern:** ^([0]|[1-9]|[1-9][0-9]|[1-9][0-9][0-9]|[1-9][0-9][0-9][0-9]|10000)$
limit	No	Integer	Specifies the page size. Minimum: **1** Maximum: **100** Default: **10** **Regex Pattern:** ^([1-9]|[1-9][0-9]|100)$

Request Parameters

Table 5-17 Request header parameters

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

Response Parameters

Status code: 200

Table 5-18 Response body parameters

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

Table 5-19 Dimension

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

Status code: 400

Table 5-20 Response body parameters

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

Status code: 500

Table 5-21 Response body parameters

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

Example Requests

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

Example Responses

Status code: 200

Query succeeded.

```
{
  "resources" : [ [ {
    "name" : "disk_name"
  } ] ],
  "count" : 10
}
```

Status Codes

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

Error Codes

See **Error Codes**.

5.2 Alarm Rules

5.2.1 Creating an Alarm Rule

Function

This API is used to create an alarm rule.

URI

POST /v2/{project_id}/alarms

Table 5-22 Path Parameters

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

Request Parameters

Table 5-23 Request header parameters

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

Table 5-24 Request body parameters

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the name of an alarm rule. The name can contain 1 to 128 characters, including only letters, digits, underscores (_), and hyphens (-).
description	No	String	Provides supplementary information about the alarm rule. The description can contain 0 to 256 characters.
namespace	Yes	String	Specifies the namespace of a service. For details about the namespace of each service, see **the Namespace column**.
resource_group_id	No	String	Specifies the resource group ID. This parameter is mandatory when Monitoring Scope is set to Resource Groups.
resources	Yes	Array<Array<**Dimension**>>	Specifies the resource list. This parameter is mandatory when Monitored Scope is set to Specified Resources.
policies	Yes	Array of **Policy** objects	Alarm Policies
type	Yes	String	Specifies the alarm rule type. Enumeration values: • **EVENT.SYS** • **EVENT.CUSTOM** • **DNSHealthCheck** • **RESOURCE_GROUP** • **MULTI_INSTANCE** • **ALL_INSTANCE**
alarm_notifications	No	Array of **Notification** objects	Specifies the action to be triggered by an alarm.
ok_notifications	No	Array of **Notification** objects	Specifies the action to be triggered after the alarm is cleared.
notification_begin_time	No	String	Specifies the time when alarm notifications are enabled.

Parameter	Mandatory	Type	Description
notification_end_time	No	String	Specifies the time when alarm notifications are disabled.
enterprise_project_id	No	String	Specifies the enterprise project ID.
enabled	Yes	Boolean	Specifies whether an alarm rule is enabled.
notification_enabled	Yes	Boolean	Specifies whether to enable alarm notifications.
alarm_template_id	No	String	Specifies the ID of the alarm template associated with the alarm rule. If this parameter is specified, the policy associated with the alarm rule changes accordingly with the alarm template policy.

Table 5-25 Dimension

Parameter	Mandatory	Type	Description
name	Yes	String	Resource dimension. For example, the dimension of an ECS is instance_id. A maximum of four dimensions are supported. For the metric dimension of each resource, see **Service metric dimension**. **Regex Pattern:** ^([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_|-){1,32}$
value	No	String	Specifies the value of a resource dimension, which is the resource instance ID, for example, 4270ff17-aba3-4138-89fa-820594c39755. **Regex Pattern:** ^((([a-z]|[A-Z]|[0-9]){1}([a-z]|[A-Z]|[0-9]|_|-|\.)*)|*){1,256}$

Table 5-26 Policy

Parameter	Mandatory	Type	Description
metric_name	Yes	String	Specifies the metric name of a resource. The name must start with a letter and contain only letter, digits, and underscores (_) . The length ranges from 1 to 64 characters. For example, cpu_util of an ECS indicates the CPU usage of the ECS. mongo001_command_ps in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.
period	Yes	Integer	Specifies the monitoring period of a metric, in seconds. The default value is 0. For example, for an event alarm, set this parameter to 0. 1 indicates the original monitoring period of the metric. For example, if the original period of an RDS metric is 60s, the RDS metric is calculated every 60 seconds as a data point. For details about the original period of each cloud service metric, see **the Namespace column**. 300 indicates that the metric is calculated every 5 minutes as a data point. Minimum: **0** Maximum: **86400** Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**
filter	Yes	String	Specifies the aggregation method. The value can be average, min, max, or sum.

Parameter	Mandatory	Type	Description
comparison_operator	Yes	String	Specifies the threshold operator, which can be >, <, >=, <=, =, or ><.
value	Yes	Number	Specifies the threshold.
unit	No	String	Specifies the unit.
count	Yes	Integer	Specifies the number of counts that the threshold is met.
suppress_duration	No	Integer	Specifies the alarm suppression time, in seconds. This field corresponds to the last field of the alarm policy when an alarm rule is created on the Cloud Eye console. This field is used to avoid frequent alarms. 0 indicates that the alarm is not suppressed and an alarm is generated when the condition is met. 300 indicates that an alarm is generated every 5 minutes after the alarm triggering condition is met. Minimum: **0** Maximum: **86400** Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**
level	No	Integer	Specifies the alarm severity, which can be: 1 (critical), 2 (major), 3 (minor) or 4 (informational).

Table 5-27 Notification

Parameter	Mandatory	Type	Description
type	Yes	String	Specifies the notification type. notification indicates that notifications are sent through Simple Message Notification (SMN). **Regex Pattern:** ^(notification|autoscaling|ecsRecovery|contact|contactGroup|iecAction)$
notification_list	Yes	Array of strings	Specifies the list of objects to be notified if the alarm status changes. The value of topicUrn can be obtained from SMN. For details, see section "Querying Topics". When type is set to notification, notification_list cannot be left blank. Note: If alarm_action_enabled is set to true, alarm_actions, ok_actions, or both of them must be specified. If alarm_actions and ok_actions coexist, their notification_list values must be the same.

Response Parameters

Status code: 201

Table 5-28 Response body parameters

Parameter	Type	Description
alarm_id	String	Specifies the alarm rule ID, which starts with al and is followed by a 22-digit string consisting of letters and digits.

Status code: 400

Table 5-29 Response body parameters

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

Status code: 500

Table 5-30 Response body parameters

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

Example Requests

```
{
  "name" : "alarm-lxy-rg-RDS",
  "description" : "",
  "namespace" : "SYS.RDS",
  "type" : "RESOURCE_GROUP",
  "resources" : [ [ {
    "name" : "rds_cluster_id"
  } ] ],
  "policies" : [ {
    "metric_name" : "rds001_cpu_util",
    "period" : 1,
    "filter" : "average",
    "comparison_operator" : ">=",
```



```
    "value" : 0,
    "unit" : "%",
    "count" : 1,
    "suppress_duration" : 86400,
    "level" : 2
  } ],
  "enabled" : true,
  "notification_enabled" : false,
  "resource_group_id" : "rg1623429506587NbRweoa3J",
  "enterprise_project_id" : "a9d919b7-0456-4bb8-b470-6a23b64f4f7e",
  "alarm_template_id" : "at1628592157541dB1klWgY6"
}
```

Example Responses

Status code: 201

Alarm rule created.

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

Status Codes

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

Error Codes

See **Error Codes**.

5.2.2 Deleting Alarm Rules in Batches

Function

This API is used to batch delete alarm rules.

URI

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

Table 5-31 Path Parameters

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

Request Parameters

Table 5-32 Request header parameters

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

Table 5-33 Request body parameters

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

Response Parameters

Status code: 200

Table 5-34 Response body parameters

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

Status code: 400

Table 5-35 Response body parameters

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

Status code: 500

Table 5-36 Response body parameters

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

Example Requests

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

Example Responses

Status code: 200

Alarm rules deleted.

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

Status Codes

Status Code	Description
200	Alarm rules deleted.
400	Parameter verification failed.
500	System error.

Error Codes

See **Error Codes**.

5.2.3 Enabling or Disabling Alarm Rules in Batches

Function

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

URI

POST /v2/{project_id}/alarms/action

Table 5-37 Path Parameters

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

Request Parameters

Table 5-38 Request header parameters

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

Table 5-39 Request body parameters

Parameter	Mandatory	Type	Description
alarm_ids	Yes	Array of strings	Specifies the IDs of the alarm rules to be enabled or disabled in batches.
alarm_enabled	Yes	Boolean	Specifies whether an alarm rule is enabled.

Response Parameters

Status code: 200

Table 5-40 Response body parameters

Parameter	Type	Description
alarm_ids	Array of strings	Specifies the IDs of alarm rules that are enabled or disabled.

Status code: 400

Table 5-41 Response body parameters

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

Status code: 500

Table 5-42 Response body parameters

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

Example Requests

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

Example Responses

Status code: 200

Alarm rules enabled or disabled.


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

Status Codes

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

Error Codes

See **Error Codes**.

5.2.4 Querying Alarm Rules

Function

This API is used to querying alarm rules.

URI

GET /v2/{project_id}/alarms

Table 5-43 Path Parameters

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

Table 5-44 Query Parameters

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

Parameter	Mandatory	Type	Description
name	No	String	Specifies the name of an alarm rule. The name can contain 1 to 128 characters, including only letters, digits, underscores (_), and hyphens (-). Minimum: **1** Maximum: **128** **Regex Pattern:** ^([\u4E00-\u9FFF]|[a-z]|[A-Z]|[0-9]|_|-)+$
namespace	No	String	Specifies the namespace of a service. For details about the namespace of each service, see **the Namespace column**. Maximum: **32** **Regex Pattern:** ^((([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*\.([a-z]|[A-Z]){1}([a-z]|[A-Z]|[0-9]|_)*)|)$
resource_id	No	String	Specifies the alarm resource ID. If a resource has multiple dimensions, the resource IDs are sorted in ascending alphabetical order and separated by commas (,). Maximum: **700** **Regex Pattern:** ^([a-z]|[A-Z]|[0-9]|_|-|:|,|\.|)+$
enterprise_project_id	No	String	Specifies the enterprise project ID. **Regex Pattern:** ^((([a-z]|[0-9]){8}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){4}-([a-z]|[0-9]){12})|0)$
offset	No	Integer	Specifies the pagination offset. Minimum: **0** Maximum: **10000** Default: **0** **Regex Pattern:** ^([0]|[1-9]|[1-9][0-9]|[1-9][0-9][0-9]|[1-9][0-9][0-9][0-9]|10000)$

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the page size. Minimum: **1** Maximum: **100** Default: **10** **Regex Pattern:** ^([1-9]|[1-9][0-9]|100)$

Request Parameters

Table 5-45 Request header parameters

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

Response Parameters

Status code: 200

Table 5-46 Response body parameters

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

Table 5-47 alarms

Parameter	Type	Description
alarm_id	String	Specifies the alarm rule ID, which starts with al and is followed by a 22-digit string consisting of letters and digits.
name	String	Specifies the name of an alarm rule. The name can contain 1 to 128 characters, including only letters, digits, underscores (_), and hyphens (-).
description	String	Provides supplementary information about the alarm rule. The description can contain 0 to 256 characters.
namespace	String	Specifies the namespace of a service. For details about the namespace of each service, see **the Namespace column**.
policies	Array of **Policy** objects	Alarm Policies
resources	Array of **ResourcesInListResp** objects	Specifies the resource list. Associated resources can be obtained using the API for querying alarm rules.
type	String	Specifies the alarm rule type. Enumeration values: • **EVENT.SYS** • **EVENT.CUSTOM** • **DNSHealthCheck** • **RESOURCE_GROUP** • **MULTI_INSTANCE** • **ALL_INSTANCE**
enabled	Boolean	Specifies whether an alarm rule is enabled.
notification_enabled	Boolean	Specifies whether to enable alarm notifications.
alarm_notifications	Array of **Notification** objects	Specifies the action to be triggered by an alarm.
ok_notifications	Array of **Notification** objects	Specifies the action to be triggered after the alarm is cleared.
notification_begin_time	String	Specifies the time when alarm notifications are enabled.
notification_end_time	String	Specifies the time when alarm notifications are disabled.

Parameter	Type	Description
enterprise_project_id	String	Specifies the enterprise project ID.
alarm_template_id	String	Specifies the ID of the alarm template associated with the alarm rule. If this parameter is specified, the policy associated with the alarm rule changes accordingly with the alarm template policy.

Table 5-48 Policy

Parameter	Type	Description
metric_name	String	Specifies the metric name of a resource. The name must start with a letter and contain only letter, digits, and underscores (_) . The length ranges from 1 to 64 characters. For example, cpu_util of an ECS indicates the CPU usage of the ECS. mongo001_command_ps in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.
period	Integer	Specifies the monitoring period of a metric, in seconds. The default value is 0. For example, for an event alarm, set this parameter to 0. 1 indicates the original monitoring period of the metric. For example, if the original period of an RDS metric is 60s, the RDS metric is calculated every 60 seconds as a data point. For details about the original period of each cloud service metric, see **the Namespace column**. 300 indicates that the metric is calculated every 5 minutes as a data point. Minimum: **0** Maximum: **86400** Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**
filter	String	Specifies the aggregation method. The value can be average, min, max, or sum.

Parameter	Type	Description
comparison_operator	String	Specifies the threshold operator, which can be >, <, >=, <=, =, or ><.
value	Number	Specifies the threshold.
unit	String	Specifies the unit.
count	Integer	Specifies the number of counts that the threshold is met.
suppress_duration	Integer	Specifies the alarm suppression time, in seconds. This field corresponds to the last field of the alarm policy when an alarm rule is created on the Cloud Eye console. This field is used to avoid frequent alarms. 0 indicates that the alarm is not suppressed and an alarm is generated when the condition is met. 300 indicates that an alarm is generated every 5 minutes after the alarm triggering condition is met. Minimum: **0** Maximum: **86400** Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**
level	Integer	Specifies the alarm severity, which can be: 1 (critical), 2 (major), 3 (minor) or 4 (informational).

Table 5-49 ResourcesInListResp

Parameter	Type	Description
resource_group_id	String	Specifies the resource group ID. This parameter is available when Monitoring Scope is set to Resource Groups. **Regex Pattern:** ^rg([a-z]|[A-Z]|[0-9]){22}$

Parameter	Type	Description
resource_group_name	String	Specifies the resource group name. This parameter is available when Monitoring Scope is set to Resource Groups. Minimum: **1** Maximum: **128**
dimensions	Array of **MetricDimension** objects	Specifies the dimension information.

Table 5-50 MetricDimension

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

Table 5-51 Notification

Parameter	Type	Description
type	String	Specifies the notification type. notification indicates that notifications are sent through Simple Message Notification (SMN). **Regex Pattern:** ^(notification|autoscaling|ecsRecovery|contact|contactGroup|iecAction)$

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

Status code: 400

Table 5-52 Response body parameters

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

Status code: 500

Table 5-53 Response body parameters

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

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

Example Requests

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

Example Responses

Status code: 200

Query succeeded.

```
{
  "alarms" : [ {
    "alarm_id" : "al16558829757444BVVxr999",
    "name" : "alarm01",
    "description" : "",
    "namespace" : "SYS.ECS",
    "policies" : [ {
      "metric_name" : "disk_device_read_bytes_rate",
      "period" : 1,
      "filter" : "average",
      "comparison_operator" : ">",
      "value" : 75,
      "unit" : "byte/s",
      "count" : 3,
      "suppress_duration" : 10800,
      "level" : 2
    } ],
    "resources" : [ {
      "dimensions" : [ {
        "name" : "disk_name"
      } ]
    } ],
    "type" : "ALL_INSTANCE",
    "enabled" : true,
    "notification_enabled" : true,
    "alarm_notifications" : [ {
      "type" : "notification",
      "notification_list" : [ "urn:smn:xxx:xxx70e7359:topic_xxx" ]
    } ],
    "ok_notifications" : [ {
      "type" : "notification",
      "notification_list" : [ "urn:smn:xxx:xxx70e7359:topic_xxx" ]
    } ],
    "notification_begin_time" : "00:00",
    "notification_end_time" : "23:59",
    "enterprise_project_id" : 0
  } ]
}
```


Status Codes

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

Error Codes

See **Error Codes**.

5.3 Alarm Records

5.3.1 Querying Alarm Records

Function

This API is used to query alarm records.

URI

GET /v2/{project_id}/alarm-histories

Table 5-54 Path Parameters

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

Table 5-55 Query Parameters

Parameter	Mandatory	Type	Description
alarm_id	No	String	Specifies an alarm ID, which starts with al and is followed by a 22-digit string consisting of letters and digits. Minimum: **24** Maximum: **24**
name	No	String	Specifies the alarm rule name. Minimum: **0** Maximum: **128**
status	No	String	Specifies the alarm rule status. The value can be ok, alarm or invalid. Minimum: **0** Maximum: **64** **Regex Pattern:** ^(ok|alarm|invalid)$
level	No	Integer	Specifies the alarm severity, which can be: 1 (critical), 2 (major), 3 (minor) or 4 (informational). Minimum: **1** Maximum: **4**
namespace	No	String	Specifies the namespace of a service. For details about the namespace of each service, see **the Namespace column**. Minimum: **3** Maximum: **32**
resource_id	No	String	Specifies the alarm resource ID. If a resource has multiple dimensions, the resource IDs are sorted in ascending alphabetical order and separated by commas (,). Minimum: **0** Maximum: **2048**

Parameter	Mandatory	Type	Description
from	No	String	Specifies the start time for querying alarm records, for example, 2022-02-10T10:05:46+08:00. Minimum: **0** Maximum: **64**
to	No	String	Specifies the end time for querying alarm records, for example, 2022-02-10T10:05:47+08:00. Minimum: **0** Maximum: **64**
offset	No	Integer	Specifies the pagination offset. Minimum: **0** Maximum: **999** Default: **0** **Regex Pattern:** ^(0|[1-9]|[1-9][0-9])$
limit	No	Integer	Specifies the page size. Minimum: **1** Maximum: **100** Default: **10** **Regex Pattern:** ^([1-9]|[1-9][0-9]|100)$

Request Parameters

Table 5-56 Request header parameters

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

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

Response Parameters

Status code: 200

Table 5-57 Response body parameters

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

Table 5-58 AlarmHistoryItemV2

Parameter	Type	Description
record_id	String	Specifies the alarm record ID. Minimum: **24** Maximum: **24**
alarm_id	String	Specifies the alarm rule ID, for example, al1603131199286dzxpqK3Ez. Minimum: **24** Maximum: **24**
name	String	Specifies the alarm rule name, for example, alarm-test01. Minimum: **1** Maximum: **128**

Parameter	Type	Description
status	String	Specifies the status of an alarm record. The value can be ok, alarm, or invalid. Enumeration values: • **ok** • **alarm** • **invalid**
level	Integer	Specifies the severity of an alarm record. The value can be 1 (critical), 2 (major), 3 (minor), or 4 (informational). Enumeration values: • **1** • **2** • **3** • **4**
type	String	Specifies the alarm rule type. Enumeration values: • **EVENT.SYS** • **EVENT.CUSTOM** • **DNSHealthCheck** • **RESOURCE_GROUP** • **MULTI_INSTANCE** • **ALL_INSTANCE**
action_enabled	Boolean	Specifies whether to send a notification. The value can be true or false.
begin_time	String	Specifies when an alarm record is generated (UTC time).
end_time	String	Specifies when an alarm record becomes invalid (UTC time).
metric	**Metric** object	Specifies the metric information.
condition	**AlarmCondition** object	Specifies the alarm triggering condition.
additional_info	**AdditionalInfo** object	Specifies the additional field of an alarm record, which applies only to alarm records generated in the event monitoring scenario.

Parameter	Type	Description
alarm_actions	Array of **Notification** objects	Specifies the action to be triggered by an alarm. The structure is as follows: { "type": "notification", "notification_list": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"] }. type can be notification, autoscaling, or notification_list. notification: indicates that a notification action will be triggered. autoscaling: indicates that a scaling action will be triggered. notification_list: When the alarm rule status changes, Cloud Eye will notify users in the notification list.
ok_actions	Array of **Notification** objects	Specifies the action to be triggered after the alarm is cleared. The structure is as follows: { "type": "notification", "notification_list": ["urn:smn:southchina:68438a86d98e427e907e0097b7e35d47:sd"] }. type can be notification or notification_list. notification: indicates that a notification action will be triggered. notification_list: When the alarm rule status changes, Cloud Eye will notify users in the notification list.
data_points	Array of **DataPointInfo** objects	Specifies the time when the resource monitoring data is reported and the monitoring data in the alarm record.

Table 5-59 Metric

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

Parameter	Type	Description
metric_name	String	Specifies the metric name of a resource. The name must start with a letter and contain only letters, digits, and underscores (_). The length ranges from 1 to 64 characters. For example, cpu_util of an ECS indicates the CPU usage of the ECS. mongo001_command_ps in Distribute Data Service (DDS) indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**. Minimum: **1** Maximum: **64**
dimensions	Array of **Dimension** objects	Specifies the metric dimension. A maximum of four dimensions can be added.

Table 5-60 Dimension

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

Table 5-61 AlarmCondition

Parameter	Type	Description
period	Integer	Specifies the monitoring period of a metric, in seconds. The default value is 0. For example, for an event alarm, set this parameter to 0. 1 indicates the original monitoring period of the metric. For example, if the original period of an RDS metric is 60s, the Relational Database Service (RDS) metric is calculated every 60 seconds as a data point. For details about the original period of each cloud service metric, see **the Namespace column**. 300 indicates that the metric is calculated every 5 minutes as a data point. Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**
filter	String	Specifies the aggregation method. The value can be average, min, max, or sum. Minimum: **1** Maximum: **15** **Regex Pattern:** ^(average|min|max|sum)$
comparison_operator	String	Specifies the threshold operator. Minimum: **1** Maximum: **10** **Regex Pattern:** ^(>|<|>=|<=|=)$
value	Double	Specifies the alarm threshold. Supported range: 0 to Number. MAX_VALUE (1.7976931348623157e+108) For detailed thresholds, see the value range of each metric in the appendix. For example, you can set Elastic Cloud Server (ECS) cpu_util to 80. Minimum: **0** Maximum: **1.174271E108**
unit	String	Specifies the data unit. Enter up to 32 characters. Minimum: **0** Maximum: **32**

Parameter	Type	Description
count	Integer	Specifies the number of counts that the threshold is met. Minimum: **1** Maximum: **100**
suppress_duration	Integer	Specifies the alarm suppression time, in seconds. This field corresponds to the last field of the alarm policy when an alarm rule is created on the Cloud Eye console. This field is used to avoid frequent alarms. 0 indicates that the alarm is not suppressed and an alarm is generated when the condition is met. 300 indicates that an alarm is generated every 5 minutes after the alarm triggering condition is met. Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** **Regex Pattern:** ^(0|300|600|900|1800|3600|10800|21600|43200|86400)$

Table 5-62 AdditionalInfo

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

Parameter	Type	Description
event_id	String	Specifies the ID of the event in the alarm record, which is the event generated by the resource, for example, ev16031292300990kKN8p17. Minimum: **24** Maximum: **24**

Table 5-63 Notification

Parameter	Type	Description
type	String	Specifies the notification type. notification indicates that notifications are sent through Simple Message Notification (SMN). **Regex Pattern:** ^(notification|autoscaling|ecsRecovery|contact|contactGroup|iecAction)$
notification_list	Array of strings	Specifies the list of objects to be notified if the alarm status changes. The value of topicUrn can be obtained from SMN. For details, see section "Querying Topics". When type is set to notification, notification_list cannot be left blank. Note: If alarm_action_enabled is set to true, alarm_actions, ok_actions, or both of them must be specified. If alarm_actions and ok_actions coexist, their notification_list values must be the same.

Table 5-64 DataPointInfo

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

Status code: 400

Table 5-65 Response body parameters

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

Status code: 500

Table 5-66 Response body parameters

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

Example Requests

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

Example Responses

Status code: 200

Query succeeded.

```
{
  "alarm_histories" : [ {
```



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


Status Codes

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

Error Codes

See **Error Codes**.

5.4 Alarm Policies

5.4.1 Modifying Alarm Policies

Function

This API is used to modify alarm policies.

URI

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

Table 5-67 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: **1** Maximum: **64** **Regex Pattern:** ^[a-zA-Z0-9-]{1,64}$
alarm_id	Yes	String	Specifies the ID of the instance for which the alarm rule is configured. **Regex Pattern:** ^al([0-9A-Za-z]){22}$

Request Parameters

Table 5-68 Request header parameters

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

Table 5-69 Request body parameters

Parameter	Mandatory	Type	Description
policies	Yes	Array of **Policy** objects	Specifies the policy information.

Table 5-70 Policy

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

Parameter	Mandatory	Type	Description
period	Yes	Integer	Specifies the monitoring period of a metric, in seconds. The default value is 0. For example, for an event alarm, set this parameter to 0. 1 indicates the original monitoring period of the metric. For example, if the original period of an RDS metric is 60s, the RDS metric is calculated every 60 seconds as a data point. For details about the original period of each cloud service metric, see **the Namespace column**. 300 indicates that the metric is calculated every 5 minutes as a data point. Minimum: **0** Maximum: **86400** Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**
filter	Yes	String	Specifies the aggregation method. The value can be average, min, max, or sum.
comparison_operator	Yes	String	Specifies the threshold operator, which can be >, <, >=, <=, =, or ><.
value	Yes	Number	Specifies the threshold.
unit	No	String	Specifies the unit.
count	Yes	Integer	Specifies the number of counts that the threshold is met.

Parameter	Mandatory	Type	Description
suppress_duration	No	Integer	Specifies the alarm suppression time, in seconds. This field corresponds to the last field of the alarm policy when an alarm rule is created on the Cloud Eye console. This field is used to avoid frequent alarms. 0 indicates that the alarm is not suppressed and an alarm is generated when the condition is met. 300 indicates that an alarm is generated every 5 minutes after the alarm triggering condition is met. Minimum: **0** Maximum: **86400** Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**
level	No	Integer	Specifies the alarm severity, which can be: 1 (critical), 2 (major), 3 (minor) or 4 (informational).

Response Parameters

Status code: 200

Table 5-71 Response body parameters

Parameter	Type	Description
policies	Array of **Policy** objects	Specifies the policy information.

Table 5-72 Policy

Parameter	Type	Description
metric_name	String	Specifies the metric name of a resource. The name must start with a letter and contain only letter, digits, and underscores (_) . The length ranges from 1 to 64 characters. For example, cpu_util of an ECS indicates the CPU usage of the ECS. mongo001_command_ps in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.
period	Integer	Specifies the monitoring period of a metric, in seconds. The default value is 0. For example, for an event alarm, set this parameter to 0. 1 indicates the original monitoring period of the metric. For example, if the original period of an RDS metric is 60s, the RDS metric is calculated every 60 seconds as a data point. For details about the original period of each cloud service metric, see **the Namespace column**. 300 indicates that the metric is calculated every 5 minutes as a data point. Minimum: **0** Maximum: **86400** Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**
filter	String	Specifies the aggregation method. The value can be average, min, max, or sum.
comparison_operator	String	Specifies the threshold operator, which can be >, <, >=, <=, =, or ><.
value	Number	Specifies the threshold.
unit	String	Specifies the unit.
count	Integer	Specifies the number of counts that the threshold is met.

Parameter	Type	Description
suppress_duration	Integer	Specifies the alarm suppression time, in seconds. This field corresponds to the last field of the alarm policy when an alarm rule is created on the Cloud Eye console. This field is used to avoid frequent alarms. 0 indicates that the alarm is not suppressed and an alarm is generated when the condition is met. 300 indicates that an alarm is generated every 5 minutes after the alarm triggering condition is met. Minimum: **0** Maximum: **86400** Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**
level	Integer	Specifies the alarm severity, which can be: 1 (critical), 2 (major), 3 (minor) or 4 (informational).

Status code: 400

Table 5-73 Response body parameters

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

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

Status code: 500

Table 5-74 Response body parameters

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

Example Requests

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

Example Responses

Status code: 200

Alarm policy modified.

```
{
  "policies" : [ {
    "metric_name" : "disk_device_read_bytes_rate",
    "period" : 1,
    "filter" : "average",
    "comparison_operator" : ">",
```

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

Status Codes

Status Code	Description
200	Alarm policy modified.
400	Parameter verification failed.
500	System error.

Error Codes

See **Error Codes**.

5.4.2 Querying Alarm Policies

Function

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

URI

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

Table 5-75 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the tenant ID. Minimum: **1** Maximum: **64** **Regex Pattern:** ^[a-zA-Z0-9-]{1,64}$
alarm_id	Yes	String	Specifies the alarm rule ID. **Regex Pattern:** ^al([0-9A-Za-z]){22}$

Table 5-76 Query Parameters

Parameter	Mandatory	Type	Description
offset	No	Integer	Specifies the pagination offset. Minimum: **0** Maximum: **10000** Default: **0** **Regex Pattern:** ^([0]|[1-9]|[1-9][0-9]|[1-9][0-9][0-9]|[1-9][0-9][0-9][0-9]|10000)$
limit	No	Integer	Specifies the page size. Minimum: **1** Maximum: **100** Default: **10** **Regex Pattern:** ^([1-9]|[1-9][0-9]|100)$

Request Parameters

Table 5-77 Request header parameters

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

Response Parameters

Status code: 200

Table 5-78 Response body parameters

Parameter	Type	Description
policies	Array of **Policy** objects	Specifies the policy information.
count	Integer	Specifies total number of policies corresponding to the specified alarm rule. Minimum: **0** Maximum: **100**

Table 5-79 Policy

Parameter	Type	Description
metric_name	String	Specifies the metric name of a resource. The name must start with a letter and contain only letter, digits, and underscores (_) . The length ranges from 1 to 64 characters. For example, cpu_util of an ECS indicates the CPU usage of the ECS. mongo001_command_ps in DDS indicates the command execution frequency. For details about the metric name of each service, see **Service metric name**.
period	Integer	Specifies the monitoring period of a metric, in seconds. The default value is 0. For example, for an event alarm, set this parameter to 0. 1 indicates the original monitoring period of the metric. For example, if the original period of an RDS metric is 60s, the RDS metric is calculated every 60 seconds as a data point. For details about the original period of each cloud service metric, see **the Namespace column**. 300 indicates that the metric is calculated every 5 minutes as a data point. Minimum: **0** Maximum: **86400** Enumeration values: • **0** • **1** • **300** • **1200** • **3600** • **14400** • **86400**

Parameter	Type	Description
filter	String	Specifies the aggregation method. The value can be average, min, max, or sum.
comparison_operator	String	Specifies the threshold operator, which can be >, <, >=, <=, =, or ><.
value	Number	Specifies the threshold.
unit	String	Specifies the unit.
count	Integer	Specifies the number of counts that the threshold is met.
suppress_duration	Integer	Specifies the alarm suppression time, in seconds. This field corresponds to the last field of the alarm policy when an alarm rule is created on the Cloud Eye console. This field is used to avoid frequent alarms. 0 indicates that the alarm is not suppressed and an alarm is generated when the condition is met. 300 indicates that an alarm is generated every 5 minutes after the alarm triggering condition is met. Minimum: **0** Maximum: **86400** Enumeration values: • **0** • **300** • **600** • **900** • **1800** • **3600** • **10800** • **21600** • **43200** • **86400**
level	Integer	Specifies the alarm severity, which can be: 1 (critical), 2 (major), 3 (minor) or 4 (informational).

Status code: 400

Table 5-80 Response body parameters

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

Status code: 404

Table 5-81 Response body parameters

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

Status code: 500

Table 5-82 Response body parameters

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

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

Example Requests

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

Example Responses

Status code: 200

Query succeeded.

```
{
  "policies" : [ {
    "metric_name" : "disk_device_read_bytes_rate",
    "period" : 1,
    "filter" : "average",
    "comparison_operator" : ">",
    "value" : 75,
    "unit" : "byte/s",
    "count" : 3,
    "suppress_duration" : 10800,
    "level" : 2
  } ],
  "count" : 10
}
```

Status Codes

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

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 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.

You can grant users permissions by using roles and policies. A policy consists of permissions for an entire service. Users with such a policy assigned are granted all of the permissions required for that service. Policies define API-based permissions for operations on specific resources, allowing for more fine-grained, secure access control of cloud resources.

NOTE

If you want to allow or deny the access to an API, use policies for authorization.

An account has permissions to call all APIs. An IAM user under the account can call specific APIs only after being assigned the required permissions. The permissions required for calling an API are determined by the actions supported by the API. Only users who have been granted permissions allowing the actions can call the API successfully. For example, if an IAM user queries the alarm rule list using an API, the user must have been granted permissions that allow the **ces:alarms:list** action.

Supported Actions

Cloud Eye provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- Permissions: Defined by actions in a custom policy.
- Actions: Added to a custom policy to control permissions for specific operations.
- Related actions: Actions on which a specific action depends to take effect. When assigning permissions for the action to a user, you also need to assign permissions for the dependent actions.
- Authorization Scope: A custom policy can be applied to IAM projects or enterprise projects or both. Policies that contain actions supporting both IAM and enterprise projects can be assigned to user groups and take effect in both IAM and Enterprise Management. Policies that only contain actions supporting IAM projects can be assigned to user groups and only take effect for IAM. Such policies will not take effect if they are assigned to user groups in Enterprise Management.
- APIs: REST APIs that can be called in a custom policy

Cloud Eye supports the following actions that can be defined in custom policies:

NOTE

√ indicates that the item is supported, and × indicates that the item is not supported.

Supported Actions of the API Version Management APIs

Supported Actions of the Metric Management API

Supported Actions of the Alarm Rule Management APIs

Supported Actions of the Monitoring Data Management APIs

Supported Actions of the Quota Management API

Supported Actions of the Event Monitoring API

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 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 (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 the project ID by calling the IAM API used to query project information based on the 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 **My Credentials** page, view the project ID (value in the **Project ID** column).

A Appendix

A.1 Services Interconnected with Cloud Eye

Category	Service	Namespace	Reference
Compute	Elastic Cloud Server	SYS.ECS	ECS metrics
	ECS (OS monitoring)	AGT.ECS	ECS Metrics Under OS Monitoring (with Agent Installed)
	Auto Scaling	SYS.AS	AS metrics
Storage	Elastic Volume Service	SYS.EVS	EVS metrics
	Object Storage Service	SYS.OBS	OBS metrics
	Scalable File Service	SYS.SFS	SFS metrics
Network	Elastic IP and bandwidth	SYS.VPC	VPC metrics
	Elastic Load Balance	SYS.ELB	ELB metrics
	NAT Gateway	SYS.NAT	NAT Gateway metrics
Application	Distributed Message Service	SYS.DMS	DMS metrics (Kafka) DMS metrics (RabbitMQ)
	Distributed Cache Service	SYS.DCS	DCS metrics

Category	Service	Namespace	Reference
Database	Relational Database Service	SYS.RDS	RDS for MySQL metrics RDS for PostgreSQL metrics
	Document Database Service	SYS.DDS	DDS metrics
Enterprise Intelligence	Cloud Search Service	SYS.ES	CSS metrics

A.2 Events Supported by Event Monitoring

Table A-1 Elastic Cloud Server (ECS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
ECS	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.
	Restart triggered due to hardware fault	startAutoRecovery	Major	ECSs on a faulty host would be automatically migrated to another properly-running host. During the migration, the ECSs was restarted.	Wait for the event to end and check whether services are affected.	Services may be interrupted.
	Restart completed due to hardware failure	endAutoRecovery	Major	The ECS was recovered after the automatic migration.	This event indicates that the ECS has recovered and been working properly.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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.
	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 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. For details, see *Cloud Trace Service User Guide*.	• Check whether the restart was performed intentionally by a user. • Deploy service applications in HA mode. • After the ECS starts up, check whether services recover.	Services are interrupted.

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

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	ECS resized	resizeServer	Minor	The ECS 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
	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.
	Live migration started	liveMigrationStarted	Major	The host where the ECS is located may be faulty. Live migrate the ECS in advance to prevent service interruptions caused by host breakdown.	Wait for the event to end and check whether services are affected.	Services may be interrupted for less than 1s.
	Live migration completed	liveMigrationCompleted	Major	The live migration is complete, and the ECS is running properly.	Check whether services are running properly.	None
	Live migration failure	liveMigrationFailed	Major	An error occurred during the live migration of an ECS.	Check whether services are running properly.	There is a low probability that services are interrupted.

NOTE

Once a physical host running ECSs breaks down, the ECSs are automatically migrated to a functional physical host. During the migration, the ECSs will be restarted.

Table A-2 Bare Metal Server (BMS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
BMS	BMS restarted	osReboot	Major	The BMS was restarted • on the management console. • by calling APIs.	• Deploy service applications in HA mode. • After the BMS is restarted, check whether services recover.	Services are interrupted.
	Unexpected restart	serverReboot	Major	The BMS restarted unexpectedly, which may be caused by • OS faults. • hardware faults.	• Deploy service applications in HA mode. • After the BMS is restarted, check whether services recover.	Services are interrupted.
	BMS stopped	osShutdown	Major	The BMS was stopped • on the management console. • by calling APIs.	• Deploy service applications in HA mode. • After the BMS is restarted, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Unexpected shutdown	serverShutdown	Major	The BMS was stopped unexpectedly, which may be caused by • unexpected power-off. • hardware faults.	• Deploy service applications in HA mode. • After the BMS is restarted, check whether services recover.	Services are interrupted.
	Network disconnection	linkDown	Major	The BMS network was disconnected. Possible causes are as follows: • The BMS was stopped or restarted unexpectedly. • The switch was faulty. • The gateway was faulty.	• Deploy service applications in HA mode. • After the BMS is restarted, check whether services recover.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	PCIe error	pcieError	Major	The PCIe device or main board on the BMS was faulty, which may be caused by • main board faults. • PCIe device faults.	• Deploy service applications in HA mode. • After the BMS is started, check whether services recover.	The network or disk read/write services are affected.
	Disk fault	diskError	Major	The hard disk backplane or the hard disk on the BMS is faulty. Possible causes are as follows: • Disk backplane faults • Disk faults	• Deploy service applications in HA mode. • After the fault is rectified, check whether services recover.	Data read/write services are affected, or the BMS cannot be started.
	EVS error	storageError	Major	The BMS failed to connect to EVS disks. Possible causes are as follows: • The SDI card was faulty. • Remote storage devices were faulty.	• Deploy service applications in HA mode. • After the fault is rectified, check whether services recover.	Data read/write services are affected, or the BMS cannot be started.

Table A-3 Elastic IP (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 (byte/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 (byte/s) **ingressDropBandwidth**: dropped inbound packets (bytes)		
	EIP released	deleteEip	Minor	The EIP was released.	Check whether the EIP was release by mistake.	The server that has the EIP bound cannot access the Internet.
	EIP blocked	blockEIP	Critical	The used bandwidth of an EIP exceeded 5 Gbit/s, the EIP were blocked and packets were discarded. Such an event may be caused by DDoS attacks.	Replace the EIP to prevent services from being affected. Locate and deal with the fault.	Services are impacted.
	EIP unblocked	unblockEIP	Critical	The EIP was unblocked.	Use the previous EIP again.	None
	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 (byte/s) **ingressAcceptBandwidth**: accepted inbound packets (bytes) **ingressMaxBandwidthPerSec**: peak inbound bandwidth (byte/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-4 Elastic IP (EIP)

Event Source	Event Name	Event ID	Event Severity
EIP	EIP released	deleteEip	Minor

Table A-5 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.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Domain name scheduling event	domainNameDispatchEvents	Major	The high-defense CNAME corresponding to the domain name is scheduled, and the domain name is resolved to another high-defense IP address.	Pay attention to the workloads involving the domain name.	Services are not affected.
	Blackhole event	blackHoleEvents	Major	The attack traffic exceeds the purchased AAD protection threshold.	A blackhole is canceled after 30 minutes by default. The actual blackhole duration is related to the blackhole triggering times and peak attack traffic on the current day. The maximum duration is 24 hours. If you need to permit access before a blackhole becomes ineffective, contact technical support.	Services may be interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Cancel Blackhole	cancelBlackHole	Informational	The customer's AAD instance recovers from the black hole state.	This is only a prompt and no action is required.	Customer services recover.

Table A-6 Cloud Backup and Recovery (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.
	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.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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
	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 cloud service platform.	Backup tasks may fail.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Client online	agentOnline	Major	The backup client was online.	None	None

Table A-7 Relational Database Service (RDS) — resource exception

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
RDS	DB instance creation failure	createInstanceFailed	Major	A DB instance fails to create because the number of disks is insufficient, the quota is insufficient, or underlying resources are exhausted.	Check the number and quota of disks. Release resources and create DB instances again.	DB instances cannot be created.
	Full backup failure	fullBackupFailed	Major	A single full backup failure does not affect the files that have been successfully backed up, but prolong the incremental backup time during the point-in-time restore (PITR).	Create a manual backup again.	Backup failed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Primary/standby switchover or failure	activeStandBySwitchFailed	Major	The standby DB instance does not take over workloads from the primary DB instance due to network or server failures. The original primary DB instance continues to provide workloads within a short time.	Check whether the connection between your application and the database is re-established.	None
	Replication status abnormal	abnormalReplicationStatus	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 processed. During peak hours, data may be blocked. 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 status recovered	replicationStatusRecovered	Major	The replication delay between the primary and standby instances is within the normal range, or the network connection between them has restored.	No action is required.	None
	DB instance faulty	faultyDBInstance	Major	A single or primary DB instance was faulty due to a disaster or a server failure.	Check whether an automated backup policy has been configured for the DB instance and submit a service ticket.	The database service may be unavailable.
	DB instance recovered	DBInstanceRecovered	Major	RDS rebuilds the standby DB instance with its high availability. After the instance is rebuilt, this event will be reported.	No action is required.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Failure of changing single DB instance to primary/ standby	singleToHaFailed	Major	A fault occurs when RDS is creating the standby DB instance or configuring replication between the primary and standby DB instances. The fault may occur because resources are insufficient in the data center where the standby DB instance is located.	Submit a service ticket.	Your applications are not affected because this event does not interrupt data read and write of the DB instance.
	Database process restarted	DatabaseProcessRestarted	Major	The database process is stopped due to insufficient memory or high load.	Log in to the Cloud Eye console. Check whether the memory usage increases sharply, the CPU usage is too high for a long time, or the storage space is insufficient. You can increase the CPU and memory specifications or optimize the service logic.	Downtime occurs. When this happens, RDS automatically restarts the database process and attempts to recover the workloads.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Instance storage full	instanceDiskFull	Major	Generally, the cause is that the data space usage is too high.	Scale up the instance.	The DB instance becomes read-only because the storage space is full, and data cannot be written to the database.
	Instance storage full recovered	instanceDiskFullRecovered	Major	The instance disk is recovered.	No action is required.	The instance is restored and supports both read and write operations.
	Kafka connection failed	kafkaConnectionFailed	Major	The network is unstable or the Kafka server does not work properly.	Check your network connection and the Kafka server status.	Audit logs cannot be sent to the Kafka server.

Table A-8 Relational Database Service (RDS) — operations

Event Source	Event Name	Event ID	Event Severity	Description
RDS	Reset administrator password	resetPassword	Major	The password of the database administrator is reset.
	Operate DB instance	instanceAction	Major	The storage space is scaled or the instance class is changed.
	Delete DB instance	deleteInstance	Minor	The DB instance is deleted.
	Modify backup policy	setBackupPolicy	Minor	The backup policy is modified.
	Modify parameter group	updateParameterGroup	Minor	The parameter group is modified.
	Delete parameter group	deleteParameterGroup	Minor	The parameter group is deleted.
	Reset parameter group	resetParameterGroup	Minor	The parameter group is reset.
	Change database port	changeInstancePort	Major	The database port is changed.
	Primary/standby switchover or failover	PrimaryStandbySwitched	Major	A switchover or failover is performed.

Table A-9 Document Database Service (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 processed. 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 is faulty due to a disaster or a server failure.	Submit a service ticket.	The database service may be unavailable.
	DB instance recovered	DDSDBInstanceRecovered	Major	If a disaster occurs, NoSQL provides an HA tool to automatically or manually rectify the fault. After the fault is rectified, this event is reported.	No action is required.	None
	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 storage space	DDSRiskyDataDiskUsage	Major	The storage space is insufficient.	Scale up storage space. For details, see section "Scaling Up Storage Space" in the corresponding user guide.	The instance is set to read-only and data cannot be written to the instance.
	Data disk expanded and being writable	DDSDataDiskUsageRecovered	Major	The capacity of a data disk has been expanded and the data disk becomes writable.	No action is required.	No adverse impact.

Table A-10 GaussDB NoSQL

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB NoSQL	DB instance creation failed	NoSQL CreateInstance Failed	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	NoSQL ResizeInstance Failed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you need to change the specifications again.	Services are interrupted.
	Node adding failed	NoSQL AddNodesFailed	Major	The underlying resources are insufficient.	Submit a service ticket. The O&M personnel will coordinate resources in the background, and then you delete the node that failed to be added and add a new node.	None
	Node deletion failed	NoSQL DeleteNodesFailed	Major	The underlying resources fail to be released.	Delete the node again.	None

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

Event Source	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.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Row size too large	LargeRowOccurs	Major	Rows that are too large may result in query timeouts and other faults like an OOM error.	1. Control the length of each column and row so that the sum of key and value lengths in each row does not exceed the preset threshold. 2. Check whether there are invalid writes or encoding resulting in large keys or values.	If there are rows that are too large, the cluster performance will deteriorate as the data volume grows.

Table A-11 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.

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

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

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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.
	EIP binding failure	TaurusBindEIPToInstanceFailed	Major	The binding task fails.	Submit a service ticket.	EIPs fail to be bound to instances.
	EIP unbinding failure	TaurusUnbindEIPFromInstanceFailed	Major	The unbinding task fails.	Submit a service ticket.	EIPs fail to be unbound from instances.
	Parameter modification failure	TaurusUpdateInstanceParameterFailed	Major	The network between the management plane and the instance is abnormal or the instance is abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Instance parameters fail to be modified.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Parameter template application failure	TaurusApplyParameterGroupToInstanceFailed	Major	The network between the management plane and instances is abnormal or the instances are abnormal.	Check the instance status and try again. If the fault persists, submit a service ticket.	Parameter templates fail to be applied to instances.
	Full backup failure	TaurusBackupInstanceFailed	Major	The network between the instance and the management plane (or the OBS) is disconnected, or the backup environment created for the instance is abnormal.	Submit a service ticket.	Backup jobs fail.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Primary/standby failover	TaurusActiveStandbySwitched	Major	When the network, physical machine, or database of the primary node is faulty, the system promotes a read replica to primary based on the failover priority to ensure service continuity.	1. Check whether the service is running properly. 2. Check whether an alarm is generated, indicating that the read replica failed to be promoted to primary.	During the failover, database connection is interrupted for a short period of time. After the failover is complete, you can reconnect to the database.
	Database read-only	NodeReadonlyMode	Major	The database supports only query operations.	Submit a service ticket.	After the database becomes read-only, write operations cannot be processed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Database read/ write	NodeReadWriteMode	Major	The database supports both write and read operations.	Submit a service ticket.	None.

Table A-12 GaussDB

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
GaussDB	Process status alarm	ProcessStatusAlarm	Major	Key processes exit, including CMS/CMA, ETCD, GTM, CN, and DN processes.	Wait until the process is automatically recovered or a primary/ standby failover is automatically performed. Check whether services are recovered. If no, contact SRE engineers.	If processes on primary nodes are faulty, services are interrupted and then rolled back. If processes on standby nodes are faulty, services are not affected.

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

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

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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.
	DB node recovered	TaurusNodeRunningStatusRecovered	Major	GaussDB(openGauss) provides an HA tool for automated or manual rectification of faults. After the fault is rectified, this event is reported.	No further action is required.	None
	DB instance creation failure	GaussDBV5CreateInstanceFailed	Major	Instances fail to be created because the quota is insufficient or underlying resources are exhausted.	Release the instances that are no longer used and try to provision them again, or submit a service ticket to adjust the quota.	DB instances cannot be created.

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

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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
	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

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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-13 Distributed Database Middleware (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.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	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-14 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 due to • 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.	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 due to • disk backplane faults. • disk faults.	Deploy service applications in HA mode. After the fault is rectified, check whether services recover.	Data read/ write services are affected, or the BMS cannot be started.
	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 O&M personnel.	The cloud phone cannot run properly even if it is restarted or reconfigured.
	GPU failed	gpuAbnormal	Critical	The GPU was faulty.	Submit a service ticket.	Services are interrupted.
	GPU recovered	gpuNormal	Informational	The GPU was running properly.	No action is required.	N/A
	Kernel crash	kernelCrash	Critical	The kernel log indicated crash.	Submit a service ticket.	Services are interrupted during the crash.
	Kernel OOM	kernelOom	Major	The kernel log indicated out of memory.	Submit a service ticket.	Services are interrupted.
	Hardware malfunction	hardwareError	Critical	The kernel log indicated Hardware Error.	Submit a service ticket.	Services are interrupted.
	PCIE error	pcieAer	Critical	The kernel log indicated PCIE Bus Error.	Submit a service ticket.	Services are interrupted.
	SCSI error	scsiError	Critical	The kernel log indicated SCSI Error.	Submit a service ticket.	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Image storage became read-only	partReadOnly	Critical	The image storage became read-only.	Submit a service ticket.	Services are interrupted.
	Image storage superblock damaged	badSuperBlock	Critical	The superblock of the file system of the image storage was damaged.	Submit a service ticket.	Services are interrupted.
	Image storage /.sharedpath/master became read-only	isuladMasterReadOnly	Critical	Mount point /.sharedpath/master of the image storage became read-only.	Submit a service ticket.	Services are interrupted.
	Cloud phone data disk became read-only	cphDiskReadOnly	Critical	The cloud phone data disk became read-only.	Submit a service ticket.	Services are interrupted.
	Cloud phone data disk superblock damaged	cphDiskBadSuperBlock	Critical	The superblock of the file system of the cloud phone data disk was damaged.	Submit a service ticket.	Services are interrupted.

Table A-15 Layer 2 Connection Gateway (L2CG)

Event Source	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-16 Elastic IP and bandwidth

Event Source	Event Name	Event ID	Event Severity
Elastic IP and bandwidth	VPC deleted	deleteVpc	Major
	VPC modified	modifyVpc	Minor
	Subnet deleted	deleteSubnet	Minor
	Subnet modified	modifySubnet	Minor
	Bandwidth modified	modifyBandwidth	Minor
	VPN deleted	deleteVpn	Major
	VPN modified	modifyVpn	Minor

Table A-17 Elastic Volume Service (EVS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
EVS	Update disk	updateVolume	Minor	Update the name and description of an EVS disk.	No further action is required.	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Expand disk	extendVolume	Minor	Expand an EVS disk.	No further action is required.	None
	Delete disk	deleteVolume	Major	Delete an EVS disk.	No further action is required.	Deleted disks cannot be recovered.
	QoS upper limit reached	reachQoS	Major	The I/O latency increases as the QoS upper limits of the disk are frequently reached and flow control triggered.	Change the disk type to one with a higher specification.	The current disk may fail to meet service requirements.

Table A-18 Identity and Access Management (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

Event Source	Event Name	Event ID	Event Severity
	Identity provider created	createIdentityProvider	Minor
	Identity provider deleted	deleteIdentityProvider	Major
	Identity provider updated	updateIdentityProvider	Minor
	Metadata updated	updateMetadata	Minor
	Security policy updated	updateSecurityPolicies	Major
	Credential added	addCredential	Major
	Credential deleted	deleteCredential	Major
	Project created	createProject	Minor
	Project updated	updateProject	Minor
	Project suspended	suspendProject	Major

Table A-19 Data Encryption Workshop (DEW)

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

Table A-20 Object Storage Service (OBS)

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

Event Source	Event Name	Event ID	Event Severity
	Bucket policy configured	setBucketPolicy	Minor

Table A-21 Cloud Eye

Event Source	Event Name	Event Severity
Cloud Eye	Agent heartbeat interruption	Major

Table A-22 DataSpace

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
DataSpace	New revision	newRevision	Minor	An updated version was released.	After receiving the notification, export the data of the updated version as required.	None.

Table A-23 Enterprise Switch

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
EnterpriseSwitch	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-24 Distributed Cache Service (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.
	Long-running Lua scripts stopped	scriptsStopped	Informational	Lua scripts that had timed out automatically stopped running.	Do not run Lua scripts that take a long time.	Long-running Lua scripts cannot be completed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Node restarted	nodeRestarted	Informational	After write operations had been performed, the node automatically restarted to stop Lua scripts that had timed out.	Do not run Lua scripts that take a long time.	Temporary data is inconsistent between the restarted node and the master node during the restart.

Table A-25 Intelligent Cloud Access (ICA)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
ICA	BGP peer disconnection	BgpPeerDisconnection	Major	The BGP peer is disconnected.	Log in to the gateway and locate the cause.	Service traffic may be interrupted.
	BGP peer connection success	BgpPeerConnectionSuccess	Major	The BGP peer is successfully connected.	None	None
	Abnormal GRE tunnel status	AbnormalGreTunnelStatus	Major	The GRE tunnel status is abnormal.	Log in to the gateway and locate the cause.	Service traffic may be interrupted.
	Normal GRE tunnel status	NormalGreTunnelStatus	Major	The GRE tunnel status is normal.	None	None
	WAN interface goes up	EquipmentWanGoingOnline	Major	The WAN interface goes online.	None	None

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	WAN interface goes down	EquipmentWanGoingOffline	Major	The WAN interface goes offline.	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.
	Intelligent enterprise gateway going online	IntelligentEnterpriseGatewayGoingOnline	Major	The intelligent enterprise gateway goes online.	None	None
	Intelligent enterprise gateway going offline	IntelligentEnterpriseGatewayGoingOffline	Major	The intelligent enterprise gateway goes offline.	Check whether the event is caused by a manual operation or device fault.	The device cannot be used.

Table A-26 Multi-Site High Availability Service (MAS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
MAS	Abnormal database instance	dbError	Major	Abnormal database instance is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	Database instance recovered	dbRecovery	Major	The database instance is recovered.	N/A	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Abnormal Redis instance	redisError	Major	Abnormal Redis instance is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	Redis instance recovered	redisRecovery	Major	The Redis instance is recovered.	N/A	Services are interrupted.
	Abnormal MongoDB database	mongodbError	Major	Abnormal MongoDB database is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	MongoDB database recovered	mongodbRecovery	Major	The MongoDB database is recovered.	N/A	Services are interrupted.
	Abnormal Elasticsearch instance	esError	Major	Abnormal Elasticsearch instance is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	Elasticsearch instance recovered	esRecovery	Major	The Elasticsearch instance is recovered.	N/A	Services are interrupted.
	Abnormal API	apiError	Major	The abnormal API is detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Services are interrupted.
	API recovered	apiRecovery	Major	The API is recovered.	N/A	Services are interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Area status changed	netChange	Major	Area status changes are detected by MAS.	Log in to the MAS console to view the cause and rectify the fault.	Network of the multi-active areas may change.

Table A-27 Resource Management Service (RMS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
RMS	Configuration noncompliance notification	configurationNoncomplianceNotification	Major	The assignment evaluation result is **Non-compliant**.	Modify the noncompliant configuration items of the resource.	None
	Configuration compliance notification	configurationComplianceNotification	Informational	The assignment evaluation result changed to be **Compliant**.	None	None

Table A-28 Cloud Storage Gateway (CSG)

Event Source	Event Name	Event ID	Event Severity	Description
CSG	Abnormal CSG process status	gatewayProcessStatusAbnormal	Major	This event is triggered when an exception occurs in the CSG process status.

Event Source	Event Name	Event ID	Event Severity	Description
	Abnormal CSG connection status	gatewayToServiceConnectAbnormal	Major	This event is triggered when no CSG status report is returned for five consecutive periods.
	Abnormal connection status between CSG and OBS	gatewayToObsConnectAbnormal	Major	This event is triggered when CSG cannot connect to OBS.
	Read-only file system	gatewayFileSystemReadOnly	Major	This event is triggered when the partition file system on CSG becomes read-only.
	Read-only file share	gatewayFileShareReadOnly	Major	This event is triggered when the file share becomes read-only due to insufficient cache disk storage space.

Table A-29 MapReduce Service (MRS)

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
MRS	DBServer Switchover	dbServerSwitchover	Minor	DBServer switchover occurs.	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	Consecutive active/standby switchovers may affect Hive service availability.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Flume Channel overflow	flumeChannelOverflow	Minor	Flume Channel overflow	Check whether the Flume channel configuration is proper and whether the service volume increases sharply.	Flume tasks cannot write data to the backend.
	NameNode Switchover	namenodeSwitchover	Minor	The NameNode switchover occurs.	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	Consecutive active/standby switchovers may cause HDFS file read/write failures.
	ResourceManager Switchover	resourceManagerSwitchover	Minor	ResourceManager Switchover	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	Consecutive active/standby switchovers may cause exceptions or even failures of YARN tasks.
	JobHistory Server Switchover	jobHistoryServerSwitchover	Minor	The JobHistoryServer switchover occurs.	Confirm with O&M personnel whether the active/standby switchover is caused by normal operations.	Consecutive active/standby switchovers may cause failures to read MapReduce task logs.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	HMaster Failover	hmasterFailover	Minor	The HMaster failover occurs.	Confirm with O&M personnel whether the active/ standby switchover is caused by normal operations.	Consecutive active/ standby switchovers may affect HBase service availability.
	Hue Failover	hueFailover	Minor	The Hue failover occurs.	Confirm with O&M personnel whether the active/ standby switchover is caused by normal operations.	The active/ standby switchover may affect the display of the HUE page.
	Impala HaProxy Failover	impalaHaProxyFailover	Minor	The Impala HaProxy switchover occurs.	Confirm with O&M personnel whether the active/ standby switchover is caused by normal operations.	Consecutive active/ standby switchovers may affect Impala service availability.
	Impala StateStore Catalog Failover	impalaStateStoreCatalogFailover	Minor	The Impala StateStoreCatalog failover occurs.	Confirm with O&M personnel whether the active/ standby switchover is caused by normal operations.	Consecutive active/ standby switchovers may affect Impala service availability.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	LdapServer Failover	ldapServerFailover	Minor	The LdapServer failover occur.	Confirm with O&M personnel whether the active/ standby switchover is caused by normal operations.	Consecutive active/ standby switchovers may affect LdapServer service availability.
	Loader Switchover	loaderSwitchover	Minor	The Loader switchover occur.	Confirm with O&M personnel whether the active/ standby switchover is caused by normal operations.	The active/ standby switchover may affect Loader service availability.
	Manager Switchover	managerSwitchover	Informational	The Manager switchover occurs.	Confirm with O&M personnel whether the active/ standby switchover is caused by normal operations.	The active/ standby Manager switchover may cause the Manager page inaccessible and abnormal values of some monitoring items.
	Job Running Failed	jobRunningFailed	Warning	A job fails to be executed.	On the **Jobs** tab page, check whether the failed task is normal.	The job fails to be executed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Job killed	jobkilled	Informational	The job is terminated.	Check whether the task is manually terminated.	The job execution process is terminated.
	Oozie Workflow Execution Failure	oozieWorkflowExecutionFailure	Minor	Oozie workflows fail to execute.	View Oozie logs to locate the failure cause.	Oozie workflows fail to execute.
	Oozie Scheduled Job Execution Failure	oozieScheduledJobExecutionFailure	Minor	Oozie scheduled tasks fail to execute.	View Oozie logs to locate the failure cause.	Oozie scheduled tasks fail to execute.
	ClickHouse service unavailable	clickHouseServiceUnavailable	Critical	The ClickHouse service is unavailable.	For details, see section "ALM-45425 ClickHouse Service Unavailable" in *MapReduce Service User Guide*.	The ClickHouse service is abnormal. Cluster operations cannot be performed on the ClickHouse service on FusionInsight Manager, and the ClickHouse service function cannot be used.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	DBService Service Unavailable	dbServiceServiceUnavailable	Critical	DBService is unavailable	For details, see section "ALM-27001 DBService Service Unavailable" in *MapReduce Service User Guide*.	The database service is unavailable and cannot provide data import and query functions for upper-layer services. As a result, service exceptions occur.
	DBService Heartbeat Interruption Between the Active and Standby Nodes	dbServiceHeartbeatInterruptionBetweentheActiveAndStandbyNodes	Major	DBService Heartbeat Interruption Between the Active and Standby Nodes	For details, see section "ALM-27003 Heartbeat Interruption Between the Active and Standby Nodes" in *MapReduce Service User Guide*.	During the DBService heartbeat interruption, only one node can provide the service. If this node is faulty, no standby node is available for failover and the service is unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Data Inconsistency Between Active and Standby DBServices	dataInconsistencyBetweenActiveAndStandbyDBServices	Critical	Data Inconsistency Between Active and Standby DBServices	For details, see section "ALM-27004 Data Inconsistency Between Active and Standby DBService" in *MapReduce Service User Guide*.	When data is not synchronized between the active and standby DBServices, the data may be lost or abnormal if the active instance becomes abnormal.
	Database Enters the Read-Only Mode	databaseEnterstheReadOnlyMode	Critical	The database enters the read-only mode.	For details, see section "ALM-27007 Database Enters the Read-Only Mode" in *MapReduce Service User Guide*.	The database enters the read-only mode, causing service data loss.
	Flume Service Unavailable	flumeServiceUnavailable	Critical	Flume Service Unavailable	For details, see section "ALM-24000 Flume Service Unavailable" in *MapReduce Service User Guide*.	Flume is running abnormally and the data transmission service is interrupted.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Flume Agent Exception	flumeAgentException	Major	Flume Agent Is Abnormal	For details, see section "ALM-24001 Flume Agent Exception" in *MapReduce Service User Guide*.	The Flume agent instance for which the alarm is generated cannot provide services properly, and the data transmission tasks of the instance are temporarily interrupted. Real-time data is lost during real-time data transmission.
	Flume Client Disconnection Alarm	flumeClientDisconnected	Major	Flume Client Disconnection Alarm	For details, see section "ALM-24003 Flume Client Interrupted" in *MapReduce Service User Guide*.	The Flume Client for which the alarm is generated cannot communicate with the Flume Server and the data of the Flume Client cannot be sent to the Flume Server.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Exception Occurs When Flume Reads Data	exceptionOccursWhenFlumeReadsData	Major	Exceptions occur when flume reads data.	For details, see section "ALM-24004 Exception Occurs When Flume Reads Data" in *MapReduce Service User Guide*.	If data is found in the data source and Flume Source continuously fails to read data, the data collection is stopped.
	Exception Occurs When Flume Transmits Data	exceptionOccursWhenFlumeTransmitsData	Major	Exceptions occur when flume transmits data.	For details, see section "ALM-24005 Exception Occurs When Flume Transmits Data" in *MapReduce Service User Guide*.	If the disk usage of Flume Channel increases continuously, the time required for importing data to a specified destination prolongs. When the disk usage of Flume Channel reaches 100%, the Flume agent process pauses.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Flume Certificate File is invalid	flumeCertificateFileIsinvalid	Major	The Flume certificate file is invalid or damaged.	For details, see section "ALM-24010 Flume Certificate File Is Invalid or Damaged" in *MapReduce Service User Guide*.	The Flume certificate file is invalid or damaged, and the Flume client cannot access the Flume server.
	Flume Certificate File is about to expire	flumeCertificateFileIsAboutToExpire	Major	The Flume certificate file is about to expire.	For details, see section "ALM-24011 Flume Certificate File Is About to Expire" in *MapReduce Service User Guide*.	The Flume certificate file is about to expire, which has no adverse impact on the system.
	Flume Certificate File is expired	flumeCertificateFileIsExpired	Major	The Flume certificate file has expired.	For details, see section "ALM-24012 Flume Certificate File Has Expired" in *MapReduce Service User Guide*.	The Flume certificate file has expired and functions are restricted. The Flume client cannot access the Flume server.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Flume MonitorServer Certificate File is invalid	flumeMonitorServerCertificateFileIsInvalid	Major	The Flume MonitorServer certificate file is invalid.	For details, see section "ALM-24013 Flume MonitorServer Certificate File Is Invalid or Damaged" in *MapReduce Service User Guide*.	The MonitorServer certificate file is invalid or damaged, and the Flume client cannot access the Flume server.
	Flume MonitorServer Certificate File is about to expire	flumeMonitorServerCertificateFileIsAboutToExpire	Major	The Flume MonitorServer certificate file is about to expire.	For details, see section "ALM-24014 Flume MonitorServer Certificate Is About to Expire" in *MapReduce Service User Guide*.	The MonitorServer certificate is about to expire, which has no adverse impact on the system.
	Flume MonitorServer Certificate File is expired	flumeMonitorServerCertificateFileIsExpired	Major	The Flume MonitorServer certificate file has expired.	For details, see section "ALM-24015 Flume MonitorServer Certificate File Has Expired" in *MapReduce Service User Guide*.	The MonitorServer certificate file has expired and functions are restricted. The Flume client cannot access the Flume server.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	HDFS Service Unavailable	hdfsServiceUnavailable	Critical	The HDFS service is unavailable.	For details, see section "ALM-14000 HDFS Service Unavailable" in *MapReduce Service User Guide*.	HDFS fails to provide services for HDFS service-based upper-layer components, such as HBase and MapReduce. As a result, users cannot read or write files.
	NameService Service Unavailable	nameServiceService Unavailable	Major	The NameService service is abnormal.	For details, see section "ALM-14010 NameService Service Is Abnormal" in *MapReduce Service User Guide*.	HDFS fails to provide services for upper-layer components based on the NameService service, such as HBase and MapReduce. As a result, users cannot read or write files.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	DataNode Data Directory Is Not Configured Properly	datanodeDataDirectoryIsNotConfiguredProperly	Major	The DataNode data directory is not configured properly.	For details, see section "ALM-14011 DataNode Data Directory Is Not Configured Properly" in *MapReduce Service User Guide*.	If the DataNode data directory is mounted on critical directories such as the root directory, the disk space of the root directory will be used up after running for a long time. This causes a system fault. If the DataNode data directory is not configured properly, HDFS performance will deteriorate.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Journalnode Is Out of Synchronization	journalnodeIsOutOfSynchronization	Major	The Journalnode data is not synchronized.	For details, see section "ALM-14012 JournalNode Is Out of Synchronization" in *MapReduce Service User Guide*.	When a JournalNode is working incorrectly, data on the node is not synchronized with that on other JournalNodes. If data on more than half of JournalNodes is not synchronized, the NameNode cannot work correctly, making the HDFS service unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Failed to Update the NameNode FsImage File	failedToUpdateTheNameNodeFsImageFile	Major	The NameNode FsImage file failed to be updated.	For details, see section "ALM-14013 Failed to Update the NameNode FsImage File" in *MapReduce Service User Guide*.	If the FsImage file in the data directory of the active NameNode is not updated, the HDFS metadata combination function is abnormal and requires rectification. If it is not rectified, the Editlog files increase continuously after HDFS runs for a period. In this case, HDFS restart is time-consuming because a large number of Editlog files need to be loaded. In addition, this alarm also indicates that the standby NameNode is abnormal and the

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
						NameNode high availability (HA) mechanism becomes invalid. When the active NameNode is faulty, the HDFS service becomes unavailable.
	DataNode Disk Fault	datanodeDiskFault	Major	The DataNode disk is faulty.	For details, see section "ALM-14027 DataNode Disk Fault" in *MapReduce Service User Guide*.	If a DataNode disk fault alarm is reported, a faulty disk partition exists on the DataNode. As a result, files that have been written may be lost.
	Yarn Service Unavailable	yarnServiceUnavailable	Critical	The Yarn service is unavailable.	For details, see section "ALM-18000 Yarn Service Unavailable" in *MapReduce Service User Guide*.	The cluster cannot provide the Yarn service. Users cannot run new applications. Submitted applications cannot be run.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	NodeManager Heartbeat Lost	nodemanagerHeartbeatLost	Major	The NodeManager heartbeat is lost.	For details, see section "ALM-18002 NodeManager Heartbeat Lost" in *MapReduce Service User Guide*.	The lost NodeManager node cannot provide the Yarn service. The number of containers decreases, so the cluster performance deteriorates.
	NodeManager Unhealthy	nodemanagerUnhealthy	Major	The NodeManager is unhealthy.	For details, see section "ALM-18003 NodeManager Unhealthy" in *MapReduce Service User Guide*.	The faulty NodeManager node cannot provide the Yarn service. The number of containers decreases, so the cluster performance deteriorates.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Yarn Application Timeout	yarnApplicationTimeout	Minor	Yarn task execution timed out.	For details, see section "ALM-18020 Yarn Task Execution Timeout" in *MapReduce Service User Guide*.	The alarm persists after task execution times out. However, the task can still be properly executed, so this alarm does not exert any impact on the system.
	MapReduce Service Unavailable	mapreduceServiceUnavailable	Critical	The MapReduce service is unavailable.	For details, see section "ALM-18021 MapReduce Service Unavailable" in *MapReduce Service User Guide*.	The cluster cannot provide the MapReduce service. For example, MapReduce cannot be used to view task logs and the log archive function is unavailable.
	Insufficient Yarn Queue Resources	insufficientYarnQueueResources	Minor	Yarn queue resources are insufficient.	For details, see section "ALM-18022 Insufficient Yarn Queue Resources" in *MapReduce Service User Guide*.	It takes long time to end an application. A new application cannot run for a long time after submission.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	HBase Service Unavailable	hbaseServiceUnavailable	Critical	The HBase service is unavailable.	For details, see section "ALM-19000 HBase Service Unavailable" in *MapReduce Service User Guide*.	Operations cannot be performed, such as reading or writing data and creating tables.
	System table path or file of HBase is missing	systemTablePathOrFileOfHBaseIsMissing	Critical	The table directories or files of the HBase System are lost.	For details, see section "ALM-19012 HBase System Table Directory or File Lost" in *MapReduce Service User Guide*.	The HBase service fails to restart or start.
	Hive Service Unavailable	hiveServiceUnavailable	Critical	The Hive service is unavailable.	For details, see section "ALM-16004 Hive Service Unavailable" in *MapReduce Service User Guide*.	Hive cannot provide data loading, query, and extraction services.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Hive Data Warehouse Is Deleted	hiveDataWarehouseIsDeleted	Critical	The Hive data warehouse is deleted.	For details, see section "ALM-16045 Hive Data Warehouse Is Deleted" in *MapReduce Service User Guide*.	If the default Hive data warehouse is deleted, databases and tables fail to be created in the default data warehouse, affecting service usage.
	Hive Data Warehouse Permission Is Modified	hiveDataWarehousePermissionIsModified	Critical	The Hive data warehouse permissions are modified.	For details, see section "ALM-16046 Hive Data Warehouse Permission Is Modified" in *MapReduce Service User Guide*.	If the permissions on the Hive default data warehouse are modified, the permissions for users or user groups to create databases or tables in the default data warehouse are affected. The permissions will be expanded or reduced.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	HiveServer has been deregistered from zookeeper	hiveServerHasBeenDeregisteredFromZookeeper	Major	HiveServer has been deregistered from zookeeper.	For details, see section "ALM-16047 HiveServer Has Been Deregistered from ZooKeeper" in *MapReduce Service User Guide*.	If Hive configurations cannot be read from ZooKeeper, HiveServer will be unavailable.
	tezlib or sparklib does not exist	tezlibOrSparklibIsNotExist	Major	The tez or spark library path does not exist.	For details, see section "ALM-16048 Tez or Spark Library Path Does Not Exist" in *MapReduce Service User Guide*.	The Hive on Tez and Hive on Spark functions are affected.
	Hue Service Unavailable	hueServiceUnavailable	Critical	The Hue service is unavailable.	For details, see section "ALM-20002 Hue Service Unavailable" in *MapReduce Service User Guide*.	The system cannot provide data loading, query, and extraction services.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Impala Service Unavailable	impalaServiceUnavailable	Critical	The Impala service is unavailable.	For details, see section "ALM-29000 Impala Service Unavailable" in *MapReduce Service User Guide*.	The Impala service is abnormal. Cluster operations cannot be performed on Impala on FusionInsight Manager, and Impala service functions cannot be used.
	Kafka Service Unavailable	kafkaServiceUnavailable	Critical	The Kafka service is unavailable.	For details, see section "ALM-38000 Kafka Service Unavailable" in *MapReduce Service User Guide*.	The cluster cannot provide the Kafka service, and users cannot perform new Kafka tasks.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Status of Kafka Default User Is Abnormal	statusOfKafkaDefaultUserIsAbnormal	Critical	The status of Kafka default user is abnormal.	For details, see section "ALM-38007 Status of Kafka Default User Is Abnormal" in *MapReduce Service User Guide*.	If the Kafka default user status is abnormal, metadata synchronization between Brokers and interaction between Kafka and ZooKeeper will be affected, affecting service production, consumption, and topic creation and deletion.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Abnormal Kafka Data Directory Status	abnormalKafkaDataDirectoryStatus	Major	The status of Kafka data directory is abnormal.	For details, see section "ALM-38008 Abnormal Kafka Data Directory Status" in *MapReduce Service User Guide*.	If the Kafka data directory status is abnormal, the current replicas of all partitions in the data directory are brought offline, and the data directory status of multiple nodes is abnormal at the same time. As a result, some partitions may become unavailable.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Topics with Single Replica	topicsWithSingleReplica	Warning	A topic with a single replica exists.	For details, see section "ALM-38010 Topics with Single Replica" in *MapReduce Service User Guide*.	There is the single point of failure (SPOF) risk for topics with only one replica. When the node where the replica resides becomes abnormal, the partition does not have a leader, and services on the topic are affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	KrbServer Service Unavailable	krbServerServiceUnavailable	Critical	The KrbServer service is unavailable.	For details, see section "ALM-25500 KrbServer Service Unavailable" in *MapReduce Service User Guide*.	When this alarm is generated, no operation can be performed for the KrbServer component in the cluster. The authentication of KrbServer in other components will be affected. The running status of components that depend on KrbServer in the cluster is faulty.
	Kudu Service Unavailable	kuduService Unavailable	Critical	The Kudu service is unavailable.	For details, see section "ALM-29100 Kudu Service Unavailable" in *MapReduce Service User Guide*.	Users cannot use the Kudu service.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	LdapServer Service Unavailable	ldapServerServiceUnavailable	Critical	The LdapServer service Is unavailable.	For details, see section "ALM-25000 LdapServer Service Unavailable" in *MapReduce Service User Guide*.	When this alarm is generated, no operation can be performed for the KrbServer users and LdapServer users in the cluster. For example, users, user groups, or roles cannot be added, deleted, or modified, and user passwords cannot be changed on the FusionInsight Manager portal. The authentication for existing users in the cluster is not affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Abnormal LdapServer Data Synchronization	abnormalLdapServerDataSynchronization	Critical	The LdapServer data synchronization is abnormal.	For details, see section "ALM-25004 Abnormal LdapServer Data Synchronization" in *MapReduce Service User Guide*.	LdapServer data inconsistency occurs because LdapServer data on Manager or in the cluster is damaged. The LdapServer process with damaged data cannot provide services externally, and the authentication functions of Manager and the cluster are affected.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Nscd Service Is Abnormal	nscdServiceIsAbnormal	Major	The Nscd service is abnormal.	For details, see section "ALM-25005 nscd Service Exception" in *MapReduce Service User Guide*.	If the Nscd service is abnormal, the node may fail to synchronize data from LdapServer. In this case, running the id command may fail to obtain data from LdapServer, affecting upper-layer services.
	Sssd Service Is Abnormal	sssdServiceIsAbnormal	Major	The Sssd service is abnormal.	For details, see section "ALM-25006 Sssd Service Exception" in *MapReduce Service User Guide*.	If the Sssd service is abnormal, the node may fail to synchronize data from LdapServer. In this case, running the id command may fail to obtain LDAP data, affecting upper-layer services.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Loader Service Unavailable	loaderServiceUnavailable	Critical	The Loader service is unavailable.	For details, see section "ALM-23001 Loader Service Unavailable" in *MapReduce Service User Guide*.	When the Loader service is unavailable, the data loading, import, and conversion functions are unavailable.
	Oozie Service Unavailable	oozieServiceUnavailable	Critical	The Oozie service is unavailable.	For details, see section "ALM-17003 Oozie Service Unavailable" in *MapReduce Service User Guide*.	The Oozie service cannot be used to submit jobs.
	Ranger Service Unavailable	rangerServiceUnavailable	Critical	The Ranger service is unavailable.	For details, see section "ALM-45275 Ranger Service Unavailable" in *MapReduce Service User Guide*.	When the Ranger service is unavailable, the Ranger cannot work properly and the native UI of the Ranger cannot be accessed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Abnormal RangerAdmin status	abnormalRangerAdminStatus	Major	The RangerAdmin status is abnormal.	For details, see section "ALM-45276 Abnormal RangerAdmin Status" in *MapReduce Service User Guide*.	If the status of a single RangerAdmin is abnormal, the access to the Ranger native UI is not affected. If the status of two RangerAdmins is abnormal, the Ranger native UI cannot be accessed and operations such as creating, modifying, and deleting policies cannot be performed.
	Spark2x Service Unavailable	spark2xServiceUnavailable	Critical	The Spark2x service is unavailable.	For details, see section "ALM-43001 Spark2x Service Unavailable" in *MapReduce Service User Guide*.	The Spark tasks submitted by users fail to be executed.

Event Source	Event Name	Event ID	Event Severity	Description	Solution	Impact
	Storm Service Unavailable	stormServiceUnavailable	Critical	The Storm service is unavailable.	For details, see section "ALM-26051 Storm Service Unavailable" in *MapReduce Service User Guide*.	The cluster cannot provide the Storm service externally, and users cannot execute new Storm tasks.
	ZooKeeper Service Unavailable	zooKeeperServiceUnavailable	Critical	The ZooKeeper service is unavailable.	For details, see section "ALM-13000 ZooKeeper Service Unavailable" in *MapReduce Service User Guide*.	ZooKeeper fails to provide coordination services for upper-layer components and the components depending on ZooKeeper may not run properly.
	Failed to Set the Quota of Top Directories of ZooKeeper Component	failedToSetTheQuotaOfTopDirectoriesOfZooKeeperComponent	Minor	The quota of top directories of ZooKeeper components failed to be configured.	For details, see section "ALM-13005 Failed to Set the Quota of Top Directories of ZooKeeper Components" in *MapReduce Service User Guide*.	Components can write a large amount of data to the top-level directory of ZooKeeper. As a result, the ZooKeeper service is unavailable.

B Change History

Released On	Description
2022-12-31	This issue is the second official release, which incorporates the following changes: Added **API v2**.
2020-08-30	This issue is the first official release.

