Storage Disaster Recovery Service

API Reference

Issue	02
Date	2023-11-20

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Before You Start

1.1 Overview

Welcome to *Storage Disaster Recovery Service API Reference*. Storage Disaster Recovery Service (SDRS) provides cross-AZ disaster recovery (DR) protection for servers. It supports recovery point objective (RPO) equal to 0, greatly reduces RD TCO for enterprises, and simplifies the DR process. If a fault occurs at the production site, you can quickly restore services at the DR site. This significantly shortens service interruptions and reduces loss.

This document describes how to use application programming interfaces (APIs) to perform operations on protection groups, protected instances, and replication pairs, and perform DR drills. For details about all supported operations, see **API Overview**.

If you plan to access SDRS through an SDRS API, ensure that you are familiar with SDRS concepts. For details, see **Overview**.

1.2 API Calling

SDRS 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**.

1.4 Constraints

- The numbers of resources that you can create are determined by your quota. To view or increase the quota, see **Managing Quotas**.
- For more constraints, see the API description.

1.5 Concepts

- Account

  An account is created upon successful registration. The account has full access permissions for all of its cloud services and resources. It can be used to reset user passwords and grant user permissions. The account is a payment entity, which should not be used directly to perform routine management. For security purposes, create Identity and Access Management (IAM) users and grant them permissions for routine management.

- User

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

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

- Region

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

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

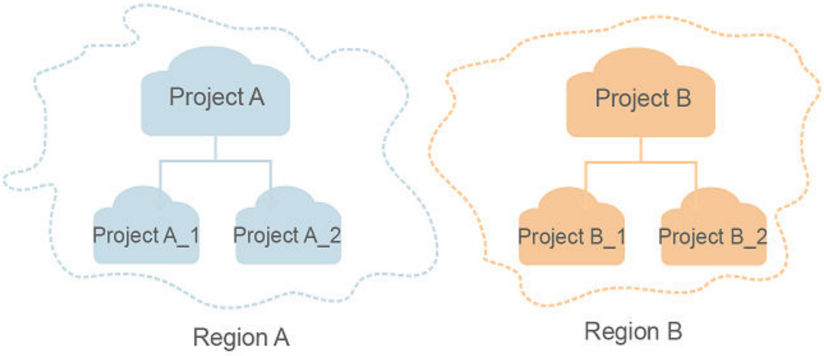
- AZ

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

- Project

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

Figure 1-1 Project isolation model



- Enterprise project

  Enterprise projects group and manage resources across regions. Resources in different enterprise projects are logically isolated. An enterprise project can contain resources of multiple regions, and resources can be added to or removed from enterprise projects.

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

2 API Overview

All SDRS APIs are extension APIs.

SDRS APIs allow you to use all SDRS functions.

Table 2-1 API section description

Section	Description
Job	After a job, such as creating or deleting a protection group, creating or deleting a protected instance, or creating or deleting a replication pair, is issued, **job_id** is returned, based on which you can query the execution status of the job.
API Version	Used to query SDRS API version information.
Active-Active Domain	An active-active domain consists of the local storage device and remote storage device. Application servers can access data across data centers using an active-active domain.
Protection Group	Used to manage a group of servers to be replicated. A protection group is for servers in one VPC. If you have multiple VPCs, you need to create multiple protection groups.
Protected Instance	A protected instance consists of a server and its replicated server. One protected instance belongs to one protection group only. Therefore, the instance servers are in the same AZs where the protection group's production site and disaster recovery site reside.
Replication Pair	A replication pair consists of one disk and its replicated disk. One replication pair belongs to one protection group and can be attached to a protected instance in this group.
DR Drill	Disaster recovery drills are used to verify that disaster recovery site servers can take over services from production site servers after a failover.
Tag Management	Tags can be used to identify and classify protected instances.

Section	Description
Task Center	Task Center allows you to manage failed tasks of all protection groups or all failed tasks of a specified protection group.
Tenant Quota Management	Used to query tenant quota information.

3 Calling APIs

3.1 Making an API Request

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

Request URI

A request URI is in the following format:

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

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

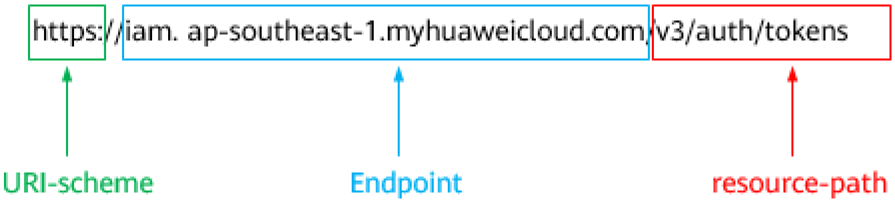
Table 3-1 URI parameter description

Parameter	Description
URI-scheme	Protocol used to transmit requests. All APIs use HTTPS.
Endpoint	Domain name or IP address of the server bearing the REST service. The endpoint varies between services in different regions. It can be obtained from **Regions and Endpoints**. For example, the endpoint of IAM in region **CN-Hong Kong** is **iam.ap-southeast-1.myhuaweicloud.com**.
resource-path	Access path of an API for performing a specified operation. Obtain the path from the URI of an API. For example, the **resource-path** of the API used to obtain a user token is **/v3/auth/tokens**.
query-string	Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of *Parameter name=Parameter value*. For example, **?limit=10** indicates that a maximum of 10 data records will be displayed.

For example, to obtain an IAM token in the **CN-Hong Kong** region, obtain the endpoint of IAM (iam.ap-southeast-1.myhuaweicloud.com) for this region and the resource-path (/v3/auth/tokens) in the URI of the API used to **obtain a user token**. Then, construct the URI as follows:

```
https://iam.ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
```

Figure 3-1 Example URI


https://iam. ap-southeast-1.myhuaweicloud.com/v3/auth/tokens
URI-scheme
Endpoint
resource-path

NOTE

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

Request Methods

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

Table 3-2 HTTP methods

Method	Description
GET	Requests the server to return specified resources.
PUT	Requests the server to update specified resources.
POST	Requests the server to add resources or perform special operations.
DELETE	Requests the server to delete specified resources, for example, an object.
HEAD	Same as GET except that the server must return only the response header.
PATCH	Requests the server to update partial content of a specified resource. If the resource does not exist, a new resource will be created.

For example, in the case of the API used to **obtain a user token**, the request method is **POST**. The request is as follows:

```
POST https://iam.ap-southeast-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
X-Project-Id	Specifies the project ID. Obtain the project ID by following the instructions in **Obtaining a Project ID**.	No This field is mandatory for requests that use AK/SK authentication in the Dedicated Cloud (DeC) scenario or multi-project scenario.	e9993fc787d94b6c886cbaa340f9c0f4

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

NOTE

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

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

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

```
POST https://iam.ap-southeast-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 (for example, JSON or XML) 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 *xxxxxxxxxxxxxxxxxx* (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.ap-southeast-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": "xxxxxxxxxxxxxxxxxx"
            }
        }
    }
}
```

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.ap-southeast-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 **Appendixes**.

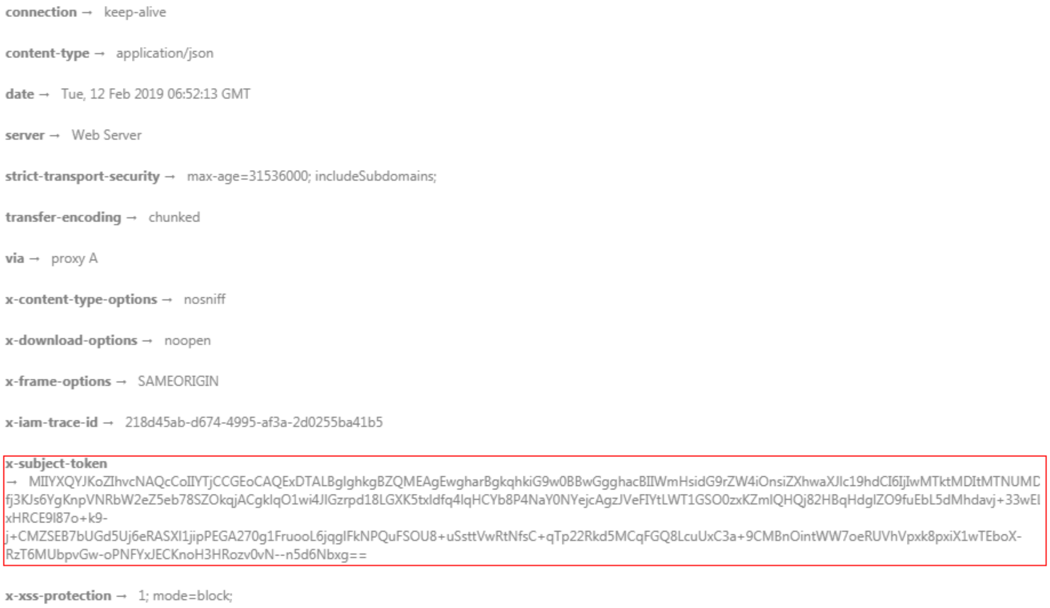
For example, if status code **201** is returned for calling the API used to **obtain a user token**, the request is successful.

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



```
connection → keep-alive

content-type → application/json

date → Tue, 12 Feb 2019 06:52:13 GMT

server → Web Server

strict-transport-security → max-age=31536000; includeSubdomains;

transfer-encoding → chunked

via → proxy A

x-content-type-options → nosniff

x-download-options → noopen

x-frame-options → SAMEORIGIN

x-iam-trace-id → 218d45ab-d674-4995-af3a-2d0255ba41b5

x-subject-token
→ MIIYXQYJKoZIhvcNAQcCoIIYTjCCGEoCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOnsiZXhwaXJlc19hdCI6IjIwMTktMDItMTNUMD
fj3KJs6YgKnpVNRbW2eZ5eb78SZOkqjACgklqO1wi4JIGzrpd18LGXK5txldfq4lqHCYb8P4NaY0NYejcAgzJVeFIYtLWT1GSO0zxKZmIQHQj82HBqHdgIZO9fuEbL5dMhdavj+33wEI
xHRCE9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXl1jipPEGA270g1FruooL6jqglFkNPQuFSOU8+uSsttVwRtNfsC+qTp22Rkd5MCqFGQ8LcuUxC3a+9CMBnOintWW7oeRUVhVpxk8pxiX1wTEboX-
RzT6MUbpvGw-oPNFYxJECKnoH3HRozv0vN--n5d6Nbxg==

x-xss-protection → 1; mode=block;
```

(Optional) Response Body

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

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

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

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

```
{
    "error_msg": "The format of message is error",
    "error_code": "AS.0001"
}
```

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

4 Getting Started

This section describes how to create a protection group by calling APIs.

NOTE

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

Involved APIs

If you use a token for authentication, you must obtain the token and add **X-Auth-Token** to the request header of the service API when making an API call.

- IAM API used to obtain the token
- SDRS API used to create a protection group

Procedure

1. Obtain the token by performing steps provided in **Authentication**.
2. Send **POST https://***SDRS endpoint***/v1/{project_id}/server-groups**.
3. Add **X-Auth-Token** to the request header.
4. Specify the following parameters in the request body:

```
{
    "server_group": {
        "name":"testname",    //Protection group name
        "description":"description",      //Protection group description
        "source_availability_zone": "az1.ac1",    //Production site AZ name of the protection group
        "target_availability_zone": "az2.ac2",    //DR site AZ name of the protection group
        "domain_id":"bccc426c-7dc4-4196-b4d8-372051f306fa",     //Active-active domain ID
        "source_vpc_id":"a9497554-3137-4a04-92bf-4be0ccdc8afe",   //Production site VPC ID
        "dr_type":"migration"     //Deployment model of the protection group
    }
}
```

   If the request is successful, a job ID is returned.

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

5. Query job details using the job ID by referring to **Querying the Job Status**.

   If the returned job status is **SUCCESS**, the protection group is successfully created.

6. Obtain the protection group ID from the body of the job. You can query, delete, or update the protection group using this ID.

5 SDRS APIs

5.1 Job

5.1.1 Querying the Job Status

Function

This API is used to query the execution status of a job.

NOTE

After a job, such as creating or deleting a protection group, creating or deleting a protected instance, and creating or deleting a replication pair, is issued, **job_id** is returned, based on which you can query the execution status of the job.

URI

- URI format

  GET /v1/{project_id}/jobs/{job_id}

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the partner ID, see **Obtaining a Project ID**.
job_id	Yes	String	Specifies the job ID. Specifies the returned parameter when the asynchronous API command is issued. For details, see the description in **Function**.

Request

- Request parameters

  None

- Example request

  GET https://{endpoint}/v1/{project_id}/jobs/0000000062db92d70162db9d200f000a

Response

- Parameter description

Parameter	Type	Description
status	String	Specifies the job status. ● **SUCCESS**: The job was successfully executed. ● **RUNNING**: The job is in progress. ● **FAIL**: The job failed. ● **INIT**: The job is being initialized.
entities	Object	Specifies the job object. The value of this parameter varies depending on the job type. If the job is a protection group-related operation, the value will be **server_group_id**. If a subjob is available, details about the subjob are displayed. For details, see **Table 5-1**.
job_id	String	Specifies the job ID. For details, see the description in **Function**.

Parameter	Type	Description
job_type	String	Specifies the job type. - **createProtectionGroupNoCG**: Creates a protection group. - **deleteProtectionGroupNoCG**: Deletes a protection group. - **startProtectionGroupNoCG**: Enables protection for a protection group. - **reprotectProtectionGroupNoCG**: Enables protection again for a protection group. - **stopProtectionGroupNoCG**: Disables protection for a protection group. - **failoverProtectionGroupNoCG**: Performs a failover for a protection group. - **reverseProtectionGroupNoCG**: Performs a planned failover for a protection group. - **createProtectedInstanceNoCG**: Creates a protected instance. - **deleteProtectedInstanceNoCG**: Deletes a protected instance. - **attachReplicationPairNew**: Attaches a replication pair to a protected instance. - **detachReplicationPairNew**: Detaches a replication pair from a protected instance. - **addNicNew**: Adds a NIC to a protected instance. - **deleteNicNew**: Deletes a NIC from a protected instance. - **resizeProtectedInstanceNew**: Modifies the specifications of a protected instance. - **createReplicationPairNoCG**: Creates a replication pair. - **deleteReplicationPairNoCG**: Deletes a replication pair. - **expandReplicationPairNew**: Expands the capacity of a replication pair. - **createDisasterRecoveryDrill**: Creates a DR drill. - **deleteDisasterRecoveryDrill**: Deletes a DR drill.

Parameter	Type	Description
begin_time	String	Specifies the start time. The default format is as follows: "yyyy-MM-dd 'T' HH:mm:ss.SSSZ", for example, **2019-04-01T12:00:00.000Z**.
end_time	String	Specifies the end time. The default format is as follows: "yyyy-MM-dd 'T' HH:mm:ss.SSSZ", for example, **2019-04-01T12:00:00.000Z**.
error_code	String	Specifies the error code returned upon a job execution failure. For details, see **Error Codes**.
fail_reason	String	Specifies the cause of a job execution failure. For details, see **Error Codes**.
message	String	Specifies the error message returned when an error occurs. For details, see the abnormal returned values in **Returned Values**.
code	String	Specifies the error code returned when an error occurs. For details, see the abnormal returned values in **Returned Values**.

Table 5-1 entities field description

Parameter	Type	Description
server_group_id	String	Specifies the ID of the protection group being queried.
sub_jobs	Array of objects	Specifies the execution information of a subjob. When no subjob exists, the value of this parameter is left empty. The structure of each subjob is similar to that of the parent job.

- Example response

```
{
    "status": "SUCCESS",
    "entities": {
        "server_group_id": "a59d008e-4bad-4bf3-9b17-6cc25e7da483"
    },
    "job_id": "0000000062db92d70162db9d200f000a",
    "job_type": "createProtectionGroupNoCG",
    "begin_time": "2018-04-19T01:55:30.443Z",
    "end_time": "2018-04-19T01:55:45.493Z",
      "error_code": null,
      "fail_reason": null
 }
```

Or

```
{
    "job_id": "ff8080826b45d4a5016b5036242c0025",
    "job_type": "stopProtectionGroupNoCG",
    "begin_time": "2019-06-13T09:40:53.930Z",
    "end_time": "2019-06-13T09:41:01.946Z",
    "status": "SUCCESS",
    "error_code": null,
    "fail_reason": null,
    "entities": {
        "sub_jobs": [
            {
                "job_id": "ff8080826b45d4a5016b50362868002a",
                "job_type": "stopProtectionGroupRepNoCG",
                "begin_time": "2019-06-13T09:40:55.015Z",
                "end_time": "2019-06-13T09:40:58.951Z",
                "status": "SUCCESS",
                "error_code": null,
                "fail_reason": null,
                "entities": {
                    "server_group_id": "1fd6903c-48f9-4772-8974-112dfbd74427"
                }
            },
            {
                "job_id": "ff8080826b45d4a5016b50362870002b",
                "job_type": "stopProtectionGroupRepNoCG",
                "begin_time": "2019-06-13T09:40:55.022Z",
                "end_time": "2019-06-13T09:40:58.952Z",
                "status": "SUCCESS",
                "error_code": null,
                "fail_reason": null,
                "entities": {
                    "server_group_id": "1fd6903c-48f9-4772-8974-112dfbd74427"
                }
            }
        ]
    }
}
{
     "error": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.

Returned Value	Description
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.2 API Version

5.2.1 Querying API Versions

Function

This API is used to query all available API versions of SDRS.

Constraints

None

URI

- URI format

  GET /

Request

- Parameter description

  None
- Example request

  GET https://{endpoint}/

Response

- Parameter description

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

Table 5-2 versions field description

Parameter	Type	Description
id	String	Specifies the version ID, for example, **v1**.
links	Array of objects	Specifies the API URL. For details, see **Table 5-3**.
version	String	Specifies the version. If the APIs of this version support microversions, the system returns the supported maximum microversion. If the microversion is not supported, the system returns an empty value.
status	String	Specifies the version status. Values are as follows: **CURRENT**: widely used version **SUPPORT**: earlier version which is still supported **DEPRECATED**: deprecated version which may be deleted later
updated	String	Specifies the version release time in UTC format. For example, the release time of v1 is 2018-05-30T15:00:00Z.

Parameter	Type	Description
min_version	String	Specifies the microversion. If APIs of a version support microversions, the system returns the supported minimum microversion. If microversions are not supported, the system returns an empty value.

Table 5-3 links parameters

Parameter	Type	Description
rel	String	Describes a link.
href	String	Specifies the version query link.

- Example response

```
{
    "versions": [
        {
            "id": "v1",
            "links": [
                {
                    "href": "https://sdrs.localdomain.com/v1",
                    "rel": "self"
                }
            ],
            "status": "CURRENT",
            "updated": "2018-05-30T15:00:00Z",
            "version": "",
            "min_version": ""
        }
    ]
}
```

Or

```
{
      "error": {
          "message": "XXXX",
          "code": "XXX"
      }
 }
```

In the preceding example, **error** indicates a general error, for example, **badrequest** or **itemNotFound**. An example is provided as follows:

```
{
      "badrequest": {
          "message": "XXXX",
          "code": "XXX"
      }
 }
```

Returned Value

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.2.2 Querying a Specified API Version

Function

This API is used to query a specified API version.

Constraints and Limitations

None

URI

- URI format

  GET /{api_version}

- Parameter description

Parameter	Mandatory	Description
api_version	Yes	Specifies the API version, for example, **v1**.

Request

- Request parameters

  None

- Example request

  GET https://{endpoint}/v1

Response

- Parameter description

Parameter	Type	Description
version	Object	Specifies the version of an API. For details, see **Table 5-4**.

Table 5-4 version field description

Parameter	Type	Description
id	String	Specifies the version ID, for example, **v1**.
links	Array of objects	Specifies the API URL. For details, see **Table 5-5**.
version	String	Specifies the version. If the APIs of this version support microversions, the system returns the supported maximum microversion. If the microversion is not supported, the system returns an empty value.

Parameter	Type	Description
status	String	Specifies the version status. Values are as follows: **CURRENT**: widely used version **SUPPORT**: earlier version which is still supported **DEPRECATED**: 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 2018-05-30T15:00:00Z.
min_version	String	Specifies the microversion. If APIs of a version support microversions, the system returns the supported minimum microversion. If microversions are not supported, the system returns an empty value.

Table 5-5 links parameters

Parameter	Type	Description
rel	String	Describes a link.
href	String	Specifies the version query link.

- Example response

```
{
    "version": {
        "id": "v1",
        "links": [
            {
                "href": "https://sdrs.localdomain.com/v1",
                "rel": "self"
            }
        ],
        "status": "CURRENT",
        "updated": "2018-05-30T00:00:00Z",
        "version": "",
        "min_version": ""
    }
}
```

Or

```
{
      "error": {
          "message": "XXXX",
          "code": "XXX"
      }
  }
```

In the preceding example, **error** indicates a general error, for example, **badrequest** or **itemNotFound**. An example is provided as follows:

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

Returned Value

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.

Returned Value	Description
504 Gateway Timeout	A gateway timeout error occurred.

5.3 Active-Active Domain

5.3.1 Querying an Active-Active Domain

Function

This API is used to query an active-active domain.

An active-active domain consists of the local storage device and remote storage device. Application servers can access data across data centers using an active-active domain.

Constraints and Limitations

None

URI

- URI format

  GET /v1/{project_id}/active-domains

- Parameter description

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

Request

- Example request

  GET https://{Endpoint}/v1/{project_id}/active-domains

Response

- Parameter description

Parameter	Type	Description
domains	Array of objects	Specifies the information about an active-active domain. For details, see **Table 5-6**.

Table 5-6 domains field description

Parameter	Type	Description
id	String	Specifies the ID of an active-active domain.
name	String	Specifies the name of an active-active domain.
description	String	Specifies the description of an active-active domain.
sold_out	Boolean	Specifies whether resources of an active-active domain are sold out.
local_replication_cluster	Object	Specifies the parameters related to the replication cluster in one AZ (either the production site AZ or DR site AZ) of the active-active domain. For details, see **Table 5-7**.
remote_replication_cluster	Object	Specifies the parameters related to replication cluster in the other AZ (either the production site AZ or DR site AZ) of the active-active domain. For details, see **Table 5-8**.

Table 5-7 local_replication_cluster field description

Parameter	Type	Description
availability_zone	String	Specifies the name of an AZ.

Table 5-8 remote_replication_cluster field description

Parameter	Type	Description
availability_zone	String	Specifies the name of an AZ.

- Example response

```
{
    "domains": [
        {
            "id": "fb4bb8e3-a574-4437-a156-78c916aeea4d",
            "name": "ActiveactiveDomain",
            "description": "my domain",
            "sold_out": false,
            "local_replication_cluster": {
                "availability_zone": "cn-north-1a"
            },
            "remote_replication_cluster": {
                "availability_zone": "cn-north-1b"
            }
        }
    ]
}
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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.

Returned Value	Description
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.4 Protection Group

5.4.1 Creating a Protection Group

Function

This API is used to create a protection group.

NOTE

This API is an asynchronous interface. If this API is invoked successfully, the request is issued. To query the creation result, invoke the API described in **Querying the Job Status**.

Constraints and Limitations

None

URI

- URI format

  POST /v1/{project_id}/server-groups
- Parameter description

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

Request

- Parameter description

Parameter	Mandatory	Type	Description
server_group	Yes	Object	Specifies the information about a protection group. For details, see **Table 5-9**.

Table 5-9 server_group field description

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the name of a protection group. The name can contain a maximum of 64 bytes. The value can contain only letters (a to z and A to Z), digits (0 to 9), decimal points (.), underscores (_), and hyphens (-).
description	No	String	Specifies the description of a protection group. The description can contain a maximum of 64 bytes. The value cannot contain the left angle bracket (<) or right angle bracket (>).
source_availability_zone	Yes	String	Specifies the production site AZ of a protection group. You can obtain this value by calling the API described in **Active-Active Domain**.
target_availability_zone	Yes	String	Specifies the DR site AZ of a protection group. You can obtain this value by calling the API described in **Active-Active Domain**.

Parameter	Mandatory	Type	Description
domain_id	Yes	String	Specifies the ID of an active-active domain. You can obtain this value by calling the API described in **Active-Active Domain**.
source_vpc_id	Yes	String	Specifies the ID of the VPC for the production site.
dr_type	No	String	Specifies the deployment model. The default value is **migration**, indicating migration within a VPC.

- Example request

  POST https://{endpoint}/v1/{project_id}/server-groups

```
{
    "server_group":
    {
        "name":"testname",
        "description":"description",
        "source_availability_zone":"cn-north-1a",
        "target_availability_zone":"cn-north-1b",
        "domain_id":"fb4bb8e3-a574-4437-a156-78c916aeea4d",
        "source_vpc_id":"046852ef-c49d-409b-8389-546aaaa5701f",
        "dr_type":"migration",

    }
}
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the job ID. Specifies the returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
   "job_id": "0000000062db92d70162db9d200f000a"
 }
```

Or

```
{
     "error": {
         "message": "XXXX",
         "code": "XXX"
```

```
    }
}
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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.

Returned Value	Description
502 Bad Gateway	Failed to complete the request because the server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.4.2 Querying Protection Groups

Function

This API is used to query all protection groups of the current tenant.

Constraints and Limitations

None

URI

- URI format

  GET /v1/{project_id}/server-groups

- Parameter description

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

- **Request filter** field description

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the maximum number of results returned each time. The value is a positive integer from 0 to 1000. The default value is **1000**.
offset	No	Integer	Specifies the offset of each request. The default value is **0**. The value must be a number and cannot be negative.

Parameter	Mandatory	Type	Description
status	No	String	Specifies the protection group status. For details, see **Protection Group Status**.
name	No	String	Specifies the name of a protection group. Fuzzy search is supported.
query_type	No	String	Specifies the query type. ● **status_abnormal**: indicates to query protection groups in the abnormal status. ● **stop_protected**: indicates to query protection groups for which the protection is disabled. ● **period_no_dr_drill**: indicates to query the protection groups for which the no DR drills have been performed in a specified duration. The default duration is 3 months. ● This parameter is invalid when the value is set to **general** or left empty.
availability_zone	No	String	Specifies the current production site AZ of a protection group. You can obtain this value by calling the API described in **Querying an Active-Active Domain**.

Request

- Request parameters

  None

- Example request

  GET https://{Endpoint}/v1/{project_id}/server-groups

Response

- Parameter description

Parameter	Type	Description
server_groups	Array of objects	Specifies the information about protection groups. For details, see **Table 5-10**.
count	Integer	Specifies the number of protection groups that meet the filtering criteria.

Table 5-10 server_groups field description

Parameter	Type	Description
id	String	Specifies the ID of a protection group.
name	String	Specifies the name of a protection group.
description	String	Specifies the description of a protection group.
status	String	Specifies the status of a protection group. For details, see **Protection Group Status**.
progress	Integer	Specifies the synchronization progress of a protection group. Unit: %
source_availability_zone	String	Specifies the production site AZ configured when a protection group is created. The value does not change after a planned failover or failover.
target_availability_zone	String	Specifies the DR site AZ configured when a protection group is created. The value does not change after a planned failover or failover.
domain_id	String	Specifies the ID of an active-active domain.
domain_name	String	Specifies the name of an active-active domain.

Parameter	Type	Description
priority_station	String	Specifies the current production site of a protection group. - **source**: indicates that the current production site AZ is the **source_availability_zone** value. - **target**: indicates that the current production site AZ is the **target_availability_zone** value.
protected_instance_num	Integer	Specifies the number of protected instances in a protection group.
replication_num	Integer	Specifies the number of replication pairs in a protection group.
disaster_recovery_drill_num	Integer	Specifies the number of DR drills in a protection group.
protected_status	String	Specifies whether protection is enabled or not. - **started**: Protection is enabled. - **stopped**: Protection is disabled. **NOTE** The system has been upgraded. For newly protection groups, the value of this parameter is **null**.
replication_status	String	Specifies the data synchronization status. - **active**: Data has been synchronized. - **inactive**: Data is not synchronized. - **copying**: Data is being synchronized. - **active-stopped**: Data synchronization is stopped. **NOTE** The system has been upgraded. For newly protection groups, the value of this parameter is **null**.
health_status	String	Specifies the health status of a protection group. - **normal**: The protection group is normal. - **abnormal**: The protection group is abnormal. **NOTE** The system is upgraded recently. For protection groups created after the upgrade, the value of this parameter is **null**.

Parameter	Type	Description
source_vpc_id	String	Specifies the ID of the VPC for the production site.
target_vpc_id	String	Specifies the ID of the VPC for the DR site.
test_vpc_id	String	Specifies the ID of the VPC used for a DR drill. This parameter is not used in the current version.
dr_type	String	Specifies the deployment model. The default value is **migration**, indicating migration within a VPC.
created_at	String	Specifies the time when a protection group was created. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.
updated_at	String	Specifies the time when a protection group was updated. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.
protection_type	String	Specifies the protection mode. ● **replication-pair**: indicates that data synchronization is performed at the replication pair level. ● **null**: indicates that data synchronization is performed at the replication consistency group level. **NOTE** The system has been upgraded. Data synchronization is performed at the replication pair level for all resources, and the returned value is **replication-pair**.
replication_model	String	Specifies the protection mode. **NOTE** This parameter is reserved.
server_type	String	Specifies the type of managed servers. ● **ECS**: indicates that ECSs are managed.

- Example response

```
{
  "count": 2,
  "server_groups": [
      {
          "id": "40df180b-9fe2-471a-8c64-1b758dc84189",
          "name": "testname",
          "description": "description",
          "source_availability_zone": "cn-north-1a",
          "target_availability_zone": "cn-north-1b",
          "domain_id": "fb4bb8e3-a574-4437-a156-78c916aeea4d",
          "domain_name": "ActiveactiveDomain",
          "status": "available",
          "protected_status": null,
          "replication_status": null,
          "health_status": null,
          "progress": 0,
          "priority_station": "source",
          "protected_instance_num": 0,
          "replication_num": 0,
          "disaster_recovery_drill_num": 0,
          "source_vpc_id": "046852ef-c49d-409b-8389-546aaaa5701f",
          "target_vpc_id": "046852ef-c49d-409b-8389-546aaaa5701f",
          "test_vpc_id": null,
          "dr_type": "migration",
          "server_type":"ECS"
          "created_at": "2019-05-23 03:51:58.256",
          "updated_at": "2019-05-23 07:48:12.484",
          "protection_type": "replication-pair",
          "replication_model": null
      },
      {
          "id": "decf224d-87fe-403a-8721-037a1a45c287",
          "name": "Protection-Group-lwx",
          "description": null,
          "source_availability_zone": "cn-north-1a",
          "target_availability_zone": "cn-north-1b",
          "domain_id": "fb4bb8e3-a574-4437-a156-78c916aeea4d",
          "domain_name": "ActiveactiveDomain",
          "status": "available",
          "protected_status": null,
          "replication_status": null,
          "health_status": null,
          "progress": 0,
          "priority_station": "source",
          "protected_instance_num": 0,
          "replication_num": 0,
          "disaster_recovery_drill_num": 0,
          "source_vpc_id": "046852ef-c49d-409b-8389-546aaaa5701f",
          "target_vpc_id": "046852ef-c49d-409b-8389-546aaaa5701f",
          "test_vpc_id": null,
          "dr_type": "migration",
          "server_type":ECS,
          "created_at": "2019-05-22 08:16:54.413",
          "updated_at": "2019-05-23 07:48:12.493",
          "protection_type": "replication-pair",
          "replication_model": null
      }
  ]
}
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.4.3 Querying the Details of a Protection Group

Function

This API is used to query the details about a protection group, such as the protection group ID and name.

Constraints and Limitations

None

URI

- URI format

  GET /v1/{project_id}/server-groups/{server_group_id}

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
server_group_id	Yes	String	Specifies the ID of a protection group. For details, see **Querying Protection Groups**.

Request

- Request parameters

  None

- Example request

  GET https://{Endpoint}/v1/{project_id}/server-groups/decf224d-87fe-403a-8721-037a1a45c287

Response

- Parameter description

Parameter	Type	Description
server_group	Object	Specifies the details of a protection group. For details, see **Table 5-11**.

Table 5-11 server_group field description

Parameter	Type	Description
id	String	Specifies the ID of a protection group.
name	String	Specifies the name of a protection group.
description	String	Specifies the description of a protection group.
status	String	Specifies the status of a protection group. For details, see **Protection Group Status**.
progress	Integer	Specifies the synchronization progress of a protection group. Unit: %
source_availability_zone	String	Specifies the production site AZ configured when a protection group is created. The value does not change after a planned failover or failover.
target_availability_zone	String	Specifies the DR site AZ configured when a protection group is created. The value does not change after a planned failover or failover.
domain_id	String	Specifies the ID of an active-active domain.
domain_name	String	Specifies the name of an active-active domain.
priority_station	String	Specifies the current production site of a protection group. ● **source**: indicates that the current production site AZ is the **source_availability_zone** value. ● **target**: indicates that the current production site AZ is the **target_availability_zone** value.
protected_instance_num	Integer	Specifies the number of protected instances in a protection group.
replication_num	Integer	Specifies the number of replication pairs in a protection group.
disaster_recovery_drill_num	Integer	Specifies the number of DR drills in a protection group.

Parameter	Type	Description
protected_status	String	Specifies whether protection is enabled or not. ● **started**: Protection is enabled. ● **stopped**: Protection is disabled. **NOTE** The system is upgraded recently. For protection groups created after the upgrade, the value of this parameter is **null**.
replication_status	String	Specifies the data synchronization status. ● **active**: Data has been synchronized. ● **inactive**: Data is not synchronized. ● **copying**: Data is being synchronized. ● **active-stopped**: Data synchronization is stopped. **NOTE** The system is upgraded recently. For protection groups created after the upgrade, the value of this parameter is **null**.
health_status	String	Specifies the health status of a protection group. ● **normal**: The protection group is normal. ● **abnormal**: The protection group is abnormal. **NOTE** The system is upgraded recently. For protection groups created after the upgrade, the value of this parameter is **null**.
source_vpc_id	String	Specifies the ID of the VPC for the production site.
target_vpc_id	String	Specifies the ID of the VPC for the DR site.
test_vpc_id	String	Specifies the ID of the VPC used for a DR drill. **NOTE** This parameter is reserved.
dr_type	String	Specifies the deployment model. The default value is **migration**, indicating migration within a VPC.

Parameter	Type	Description
created_at	String	Specifies the time when a protection group was created. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.
updated_at	String	Specifies the time when a protection group was updated. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.
protection_type	String	Specifies the protection mode. ● **null**: indicates that data synchronization is performed at the replication consistency group level. No partial synchronization failure will occur. ● **replication-pair**: indicates that data synchronization is performed at the replication pair level.
replication_model	String	Specifies the protection mode. **NOTE** This parameter is reserved.
server_type	String	Specifies the type of managed servers. ● **ECS**: indicates that ECSs are managed.

- Example response

```
{
    "server_group": {
        "id": "decf224d-87fe-403a-8721-037a1a45c287",
        "name": "Protection-Group-lwx",
        "description": null,
        "source_availability_zone": "cn-north-1a",
        "target_availability_zone": "cn-north-1b",
        "domain_id": "fb4bb8e3-a574-4437-a156-78c916aeea4d",
        "domain_name": "ActiveactiveDomain",
        "status": "available",
        "protected_status": null,
        "replication_status": null,
        "health_status": null,
        "progress": 0,
        "priority_station": "source",
        "protected_instance_num": 0,
        "replication_num": 0,
        "disaster_recovery_drill_num": 0,
        "source_vpc_id": "046852ef-c49d-409b-8389-546aaaa5701f",
        "target_vpc_id": "046852ef-c49d-409b-8389-546aaaa5701f",
        "test_vpc_id": null,
        "dr_type": "migration",
        "server_type": "ECS",
        "created_at": "2019-05-22 08:16:54.413",
        "updated_at": "2019-05-23 09:11:10.856",
        "protection_type": "replication-pair",
        "replication_model": null
    }
}
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

In the preceding example, **error** indicates a general error, for example, **badrequest** or **itemNotFound**. An example is provided as follows:

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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.

Returned Value	Description
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.4.4 Deleting a Protection Group

Function

This API is used to delete the specified protection group.

Constraints and Limitations

The protection group does not have protected instances, replication pairs, or DR drills.

NOTE

A protection group cannot be deleted if it has protected instances, replication pairs, or DR drills. To delete a protected instance, a replication pair, or a DR drill, see **Deleting a Protected Instance**, **Deleting a Replication Pair**, and **Deleting a DR Drill**.

URI

- URI format

  DELETE /v1/{project_id}/server-groups/{server_group_id}
- Parameter description

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

Parameter	Mandatory	Type	Description
server_group_id	Yes	String	Specifies the ID of a protection group. For details, see **Querying Protection Groups**.

Request

- Request parameters

  None

- Example request

  DELETE https://{Endpoint}/v1/{project_id}/server-groups/e98cefcd-2398-4a4d-8c52-c79f00e21484

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
"job_id": "0000000062db92d70162db9d200f0011"
}
```

  Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

  In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.4.5 Changing the Name of a Protection Group

Function

This API is used to change the name of a protection group.

Constraints and Limitations

None

URI

- URI format

  PUT /v1/{project_id}/server-groups/{server_group_id}

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
server_group_id	Yes	String	Specifies the ID of a protection group. For details, see **Querying Protection Groups**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
server_group	Yes	Object	Specifies the information about a protection group. For details, see **Table 5-12**.

Table 5-12 server_group field description

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the name of a protection group. ● The name can contain a maximum of 64 bytes. ● The value can contain only letters (a to z and A to Z), digits (0 to 9), decimal points (.), underscores (_), and hyphens (-).

- Example request

  PUT https://{endpoint}/v1/{project_id}/server-groups/e98cefcd-2398-4a4d-8c52-c79f00e21484

```
{
    "server_group": {
        "name": "my_test_server_group"
    }
}
```

Response

- Parameter description

Table 5-13 Parameter description

Parameter	Type	Description
server_group	Object	Specifies the details of a protection group. For details, see **Table 5-14**.

Table 5-14 server_group field description

Parameter	Type	Description
id	String	Specifies the ID of a protection group.
name	String	Specifies the name of a protection group. The name can contain a maximum of 64 bytes. The value can contain only letters (a to z and A to Z), digits (0 to 9), decimal points (.), underscores (_), and hyphens (-).
description	String	Specifies the description of a protection group.
status	String	Specifies the status of a protection group. For details, see **Protection Group Status**.
progress	Integer	Specifies the synchronization progress of a protection group. Unit: %
source_availability_zone	String	Specifies the production site AZ configured when a protection group is created. The value does not change after a planned failover or failover.

Parameter	Type	Description
target_availability_zone	String	Specifies the DR site AZ configured when a protection group is created. The value does not change after a planned failover or failover.
domain_id	String	Specifies the ID of an active-active domain.
domain_name	String	Specifies the name of an active-active domain.
protected_status	String	Specifies whether protection is enabled or not. ● **started**: Protection is enabled. ● **stopped**: Protection is disabled.
replication_status	String	Specifies the data synchronization status. ● **active**: Data has been synchronized. ● **inactive**: Data is not synchronized. ● **copying**: Data is being synchronized. ● **active-stopped**: Data synchronization is stopped.
health_status	String	Specifies the health status of a protection group. ● **normal**: The protection group is normal. ● **abnormal**: The protection group is abnormal.
priority_station	String	Specifies the current production site of a protection group. ● **source**: indicates that the current production site AZ is the **source_availability_zone** value. ● **target**: indicates that the current production site AZ is the **target_availability_zone** value.
protected_instance_num	Integer	Specifies the number of protected instances in a protection group.
replication_num	Integer	Specifies the number of replication pairs in a protection group.
disaster_recovery_drill_num	Integer	Specifies the number of DR drills in a protection group.

Parameter	Type	Description
source_vpc_id	String	Specifies the ID of the VPC for the production site.
target_vpc_id	String	Specifies the ID of the VPC for the DR site.
test_vpc_id	String	Specifies the ID of the VPC used for a DR drill.
dr_type	String	Specifies the deployment model. The default value is **migration**, indicating migration within a VPC.
server_type	String	Specifies the type of managed servers. ● **ECS**: indicates that ECSs are managed.
created_at	String	Specifies the time when a protection group was created. The default format is as follows: "yyyy-MM-dd HH:mm:ss.S", for example, **2019-04-01 12:00:00.0**.
updated_at	String	Specifies the time when a protection group was updated. The default format is as follows: "yyyy-MM-dd HH:mm:ss.S", for example, **2019-04-01 12:00:00.0**.
protection_type	String	Specifies the protection mode. ● **null**: indicates that data synchronization is performed at the replication consistency group level. No partial synchronization failure will occur. ● **replication-pair**: indicates that data synchronization is performed at the replication pair level.
replication_model	String	Specifies the protection mode. **NOTE** This parameter is reserved.

- Example response

```
{
  "server_group": {
    "id": "e98cefcd-2398-4a4d-8c52-c79f00e21484",
    "name": "my_test_server_group",
    "description": "test_server_group_sdrs",
    "status": "available",
    "progress": 0,
    "source_availability_zone": "cn-north-1a",
    "target_availability_zone": "cn-north-1b",
    "domain_id": "523ab8ad-3759-4933-9436-4cf4ebb20867",
    "domain_name": "my domain",
    "protected_status": "stopped",
    "replication_status": "active-stopped",
    "health_status": "normal",
    "priority_station": "source",
    "protected_instance_num": 0,
    "replication_num": 0,
    "disaster_recovery_drill_num": 0,
    "source_vpc_id": "ac784bd6-a79c-4def-9ff8-dc87940d5335",
    "target_vpc_id": "ac784bd6-a79c-4def-9ff8-dc87940d5335",
    "test_vpc_id": null,
    "dr_type": "migration",
    "server_type":"ECS",
    "created_at": "2018-05-09 22:11:45.0",
    "updated_at": "2018-05-09 22:11:54.0",
    "protection_type": "replication-pair",
    "replication_model": null
  }
}
```

Or

```
{
     "error": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
     "badrequest": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not find the requested page.
405 Method Not Allowed	You are not allowed to use the method specified in the request.

Returned Value	Description
406 Not Acceptable	The response generated by the server could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.4.6 Enabling Protection or Enabling Protection Again for a Protection Group

Function

This API is used to enable protection or enable protection again for a protection group.

Constraints and Limitations (Enabling Protection)

- The protection group must have replication pairs.
- **status** of the protection group must be **available** or **error-starting**.
- After you create a protected instance and enable protection on servers at the production site, modifications to the **Hostname**, **Name**, **Security Group**, **Agency**, **ECS Group**, **Tags**, and **Auto Recovery** configurations of servers on the production site will not synchronize to the servers at the DR site. You can manually add the configuration items to the servers at the DR site on the management console.

Constraints and Limitations (Enabling Protection Again)

- **status** of the protection group must be **failed-over** or **error-reprotecting**.

- Before you enable the protection again, ensure that the servers at the DR site are stopped.

URI

- URI format

  POST /v1/{project_id}/server-groups/{server_group_id}/action

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
server_group_id	Yes	String	Specifies the ID of a protection group. For details, see **Querying Protection Groups**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
start-server-group	Yes	Object	Enables protection for a protection group. This parameter is left empty.

- Example request

  POST https://{Endpoint}/v1/{project_id}/server-groups/40df180b-9fe2-471a-8c64-1b758dc84189/action

```
{
    "start-server-group": {}
}
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
    "job_id": "ff8080826adfae02016ae2d123fc05ed"
}
```

Or

```
{
     "error": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
     "badrequest": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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.

Returned Value	Description
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.4.7 Disabling Protection for a Protection Group

Function

This API is used to disable protection for a protection group.

Constraints and Limitations

- **status** of the protection group must be **protected** or **error-stopping**.

URI

- URI format

  POST /v1/{project_id}/server-groups/{server_group_id}/action

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
server_group_id	Yes	String	Specifies the ID of a protection group. For details, see **Querying Protection Groups**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
stop-server-group	Yes	Object	Disables protection for a protection group. This parameter is left empty by default.

- Example request

  POST https://{Endpoint}/v1/{project_id}/server-groups/40df180b-9fe2-471a-8c64-1b758dc84189/action

```
{
    "stop-server-group": {}
}
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
    "job_id": "ff8080826adfae02016ae2d123fc05ed"
}
```

  Or

```
{
     "error": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

  In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
     "badrequest": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.4.8 Performing a Failover for a Protection Group

Function

When the production site of a protection group becomes faulty, services of the protection group are switched over to the DR site, and servers and disks at the DR site start. After a failover is performed, the current production site of the protection group will become the DR site before the failover. Data synchronization between the production and DR sites will stop. To resume the data synchronization, you need to perform steps provided in **Enabling Protection or Enabling Protection Again for a Protection Group** to enable protection.

Constraints and Limitations

- The protection group must have replication pairs.
- **status** of the protection group must be **protected**, **error-failing-over**, or **error-reversing**.
- If the server at the production site or DR site in a protected instance is deleted using the native interface, no operations can be performed on the protected instance or the protection group of the protected instance.

URI

- URI format

  POST /v1/{project_id}/server-groups/{server_group_id}/action

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
server_group_id	Yes	String	Specifies the ID of a protection group. For details, see **Querying Protection Groups**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
failover-server-group	Yes	Object	Performs a failover for a protection group. This parameter is left empty by default.

- Example request

  POST https://{Endpoint}/v1/{project_id}/server-groups/40df180b-9fe2-471a-8c64-1b758dc84189/action

```
{
   "failover-server-group": {}
}
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
   "job_id": "ff8080826adfae02016ae2d123fc05ed"
}
```

  Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

  In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.4.9 Performing a Planned Failover for a Protection Group

Function

When you perform a planned failover for a protection group, the current production site of the protection group is switched to the DR site specified when the protection group is created, or reverse. After the planned failover is performed, data synchronization between the production site and DR site continues, but the direction is reverse.

Constraints and Limitations

- The protection group must have replication pairs.
- **status** of the protection group must be **protected** or **error-reversing**.
- All servers at the current production site of the protection group are stopped. During a planned failover, do not start servers at the production site and DR site. Otherwise, the planned failover may fail.
- If the production site server or DR site server of a protected instance is deleted using the native interface, the planned failover or planned failback will fail, and the protected instance as well as the protection group will become unavailable.

Restrictions on Logging In to a Server After You Perform a Planned Failover for the First Time

- If the production site server (when the protected instance is created) runs Windows and has Cloudbase-Init installed, pay attention to the following restrictions after you perform a planned failover for the first time:
  - If you choose to use a password for the server login, you can use the password of the production site server 3 to 5 minutes after the DR site server starts and before Cloudbase-Init starts. It takes 1 to 2 minutes for the server to display the login UI.

    After Cloudbase-Init starts, manually reset the password on the DR site server.

    After you perform a planned failback, use the configured password to log in to the production site server.
  - If you choose to use a key for the server login, you can use the password obtained from the production site server 3 to 5 minutes after the DR site server starts and before Cloudbase-Init starts. It takes 1 to 2 minutes for the server to display the login UI.

    After Cloudbase-Init starts, use the password obtained from the DR site server for the login.

    After you perform a planned failback, use the obtained password to log in to the production site server.

  NOTE

  If you change the login password of the DR site server after you perform a planned failover for the first time, log in to the DR site server using the new password. After you perform a planned failback again, use the new password to log in to the production site server.
- If the production site server (when the protected instance is created) runs Windows and has no Cloudbase-Init installed, pay attention to the following restrictions after you perform a planned failover or failover for the first time:
  - If you choose to use a password for the server login, use the password of the production site server to log in to the production site or DR site server.
  - If you choose to use a key for the server login, use the password obtained from the production site server to log in to the production site or DR site server.

- If the production site server (when the protected instance is created) runs Linux, pay attention to the following restrictions after you perform a planned failover or failover for the first time:
  - If you choose to use a password for the server login, use the password of the production site server to log in to the production site or DR site server.

    NOTE

    For servers running CoreOS, if you change the login password of the production site server after you perform a planned failover for the first time, log in to the DR site server using the new password. After you perform a planned failback again, use the initial password to log in to the production site server.
  - If you choose to use a key for the server login, use the password obtained from the production site server to log in to the production site or DR site server.

URI

- URI format

  POST /v1/{project_id}/server-groups/{server_group_id}/action
- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
server_group_id	Yes	String	Specifies the ID of a protection group. For details, see **Querying Protection Groups**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
reverse-server-group	Yes	Object	Performs a planned failover for a protection group. For details, see **Table 5-15**.

Table 5-15 reverse-server-group field description

Parameter	Mandatory	Type	Description
priority_station	Yes	String	Specifies the direction of the planned failover. ● **target**: indicates to fail services from the production site specified when the protection group is created to the DR site specified when a protection group is created. ● **source**: indicates to fail services from the DR site specified when the protection group is created to the production site specified when a protection group is created.

- Example request

  POST https://{Endpoint}/v1/{project_id}/server-groups/40df180b-9fe2-471a-8c64-1b758dc84189/action

```
{
  "reverse-server-group": {
    "priority_station": "source"
  }
}
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
   "job_id": "0000000062db92d70162db9d200f002d"
 }
```

Or

```
{
     "error": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.

Returned Value	Description
504 Gateway Timeout	A gateway timeout error occurred.

5.5 Protected Instance

5.5.1 Creating a Protected Instance

Function

This API is used to create a protected instance. When a protected instance is created, the default name of the server at the DR site is the same as that of the server at the production site, but their IDs are different. To modify a server name, click the server name on the protected instance details page to switch to the server details page and modify the server name. Alternatively, you can call the API in **Changing the Name of a Protected Instance** to modify the name.

Constraints and Limitations

- **status** of the protection group must be **available** or **protected**.
- Shared disks cannot be attached to a production site server. If you want to use a server with shared disks attached to create a protected instance, use the **API of creating protected instances in batches**.
- One server can be used to create only one protected instance.
- The server must be in the same VPC as the protection group.
- If protection is enabled for servers created during capacity expansion of an Auto Scaling (AS) group, these servers cannot be deleted when the capacity of the AS group is reduced.
- If the server at the production site runs Windows and you choose the key login mode, ensure that the key pair of the server exists when you create a protected instance. Otherwise, the server at the DR site may fail to create, causing the protected instance creation failure.

  NOTE

  If the key pair of the production site server has been deleted, create a key pair with the same name.
- If the production site server is added to Enterprise Project, the created DR site server will not be automatically added to Enterprise Project. You need to manually add it to Enterprise Project if needed.
- After you create a protected instance and enable protection on servers at the production site, modifications to the **Hostname**, **Name**, **Security Group**, **Agency**, **ECS Group**, **Tags**, and **Auto Recovery** configurations of servers on the production site will not synchronize to the servers at the DR site. You can manually add the configuration items to the servers at the DR site on the management console.

- If a production site server has been added to an ECS group, you are not allowed to specify a DeH to create the DR site server for the production site server.

URI

- URI format

  POST /v1/{project_id}/protected-instances

- Parameter description

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

Request

- Parameter description

Parameter	Mandatory	Type	Description
protected_instance	Yes	Object	Specifies the information about a protected instance. For details, see **Table 5-16**.

Table 5-16 protected_instance field description

Parameter	Mandatory	Type	Description
server_group_id	Yes	String	Specifies the ID of the protection group where a protected instance is added. For details, see **Querying Protection Groups**.
server_id	Yes	String	Specifies the ID of the production site server. **NOTE** When the API is successfully invoked, the DR site server will be automatically created.

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the name of a protected instance. The name can contain a maximum of 64 bytes. The value can contain only letters (a to z and A to Z), digits (0 to 9), decimal points (.), underscores (_), and hyphens (-).
description	No	String	Specifies the description of a protected instance. The description can contain a maximum of 64 bytes. The value cannot contain the left angle bracket (<) or right angle bracket (>).
cluster_id	No	String	Specifies the DSS storage pool ID. This parameter needs to be specified if the DR site disk uses DSS.
primary_subnet_id	No	String	Specifies the network ID of the subnet for the primary NIC on the DR site server. The value is the same as that of **neutron_network_id** obtained using the VPC API.
primary_ip_address	No	String	Specifies the IP address of the primary NIC on the DR site server. This parameter is valid only when **primary_subnet_id** is specified. If this parameter is not specified when **primary_subnet_id** is specified, the system automatically assigns an IP address to the primary NIC on the DR site server

Parameter	Mandatory	Type	Description
flavorRef	No	String	Specifies the flavor ID of the DR site server **NOTE** - If this parameter is not specified, the flavor ID of the DR site server is the same as that of the production site server by default. - Servers of different specifications have different performance, which may affect applications running on the servers. To ensure the server performance after a planned failover or failover, you are recommended to use servers of specifications (CPU and memory) same or higher than the specifications of the production site servers at the DR site.
tenancy	No	String	Specifies whether the DR site server is created on a Dedicated Host (DeH) or in a shared pool. The value can be **shared** or **dedicated**. **shared**: indicates the shared pool. **dedicated**: indicates the DeH.
dedicated_host_id	No	String	Specifies the DeH ID. This parameter takes effect only when **tenancy** is set to **dedicated**. If you do not specify this parameter, the system will automatically assign a DeH to a tenant to deploy servers.
tags	No	Array of objects	Specifies the tag list. For details, see **Table 5-17**. **NOTE** You can add up to 10 tags for each protected instance.

Table 5-17 resource_tag field description

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. The tag key of a resource must be unique. It can contain up to 36 Unicode characters. The tag key cannot be left blank or be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), equal signs (=), commas (,), vertical bars (|), and slashes (/). The tag key of a resource must be unique.
value	Yes	String	Specifies the value. It can contain up to 43 Unicode characters. The value cannot be left blank but can be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), equal signs (=), commas (,), vertical bars (|), and slashes (/).

- Example request

  POST https://{Endpoint}/v1/{project_id}/protected-instances

```
{
        "protected_instance":{
             "server_group_id": "523ab8ad-3759-4933-9436-4cf4ebb20867",
             "server_id": "403b603d-1d91-42cc-a357-81f3c2daf43f",
             "name": "test_protected_instance_name",
             "description": "my description",
             "primary_subnet_id": "a32217fh-3413-c313-6342-3124d3491502",
             "primary_ip_address": "192.168.0.5",
             "flavorRef": "s3.large.2",
             "tenancy": "dedicated",
             "dedicated_host_id": "0bc41598-1b5a-4bd2-872a-82e6abb82e68",
        }
 }
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
  "job_id": "0000000062db92d70162db9d200f00bb"
 }
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not find the requested page.
405 Method Not Allowed	You are not allowed to use the method specified in the request.

Returned Value	Description
406 Not Acceptable	The response generated by the server could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.5.2 Deleting a Protected Instance

Function

This API is used to delete a specified protected instance.

Constraints and Limitations

status of the protected instance must be **available**, **protected**, **failed-over**, **error**, **error-starting**, **error-stopping**, **error-reversing**, **error-failing-over**, **error-deleting**, **error-reprotecting**, **error-resizing**, **invalid**, or **fault**.

URI

- URI format

  DELETE /v1/{project_id}/protected-instances/{protected_instance_id}
- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
protected_instance_id	Yes	String	Specifies the ID of a protected instance. For details, see **Querying Protected Instances**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
delete_target_server	No	Boolean	Specifies whether to delete the DR site server. The default value is **false**.
delete_target_eip	No	Boolean	Specifies whether to delete the EIP of the DR site server. The default value is **false**.

- Example request

  DELETE https://{Endpoint}/v1/{project_id}/protected-instances/67a2cc7e-fb87-41a8-ba28-9c032abcaee1

```
{
  "delete_target_server": false,
  "delete_target_eip": false
}
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
  "job_id": "0000000062db92d70162db3ab00f00df"
}
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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.

Returned Value	Description
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.5.3 Querying Protected Instances

Function

This API is used to query all protected instances of the current tenant.

Constraints and Limitations

None

URI

- URI format

  GET /v1/{project_id}/protected-instances

- Parameter description

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

- **Request filter** field description

Parameter	Mandatory	Type	Description
server_group_id	No	String	Specifies the ID of the protection group, in which all protected instances are queried. For details, see the parameter description in **Querying Protection Groups**.

Parameter	Mandatory	Type	Description
server_group_ids	No	Array of strings	Specifies the protection group ID list. The value is in the following format: server_group_ids=['server_group_id1','server_group_id2',...,'server_group_idx']. Convert it using URL encoding. - All the protected instances with valid **server_group_id** in **server_group_ids** are returned. - The protected instances of a maximum of 30 **server_group_id** values can be queried. - If parameters **server_group_id** and **server_group_ids** are both specified in the request, **server_group_id** will be ignored.
protected_instance_ids	No	Array of strings	Specifies the protected instance ID list. The value is in the following format: protected_instance_ids=['protected_instance_id1','protected_instance_id2',...,'protected_instance_idx']. Convert it using URL encoding. - All the protected instances with valid **protected_instance_id** in **protected_instance_ids** are returned. - The protected instances of a maximum of 30 **protected_instance_id** values can be queried. - If parameter **server_group_id** or **server_group_ids** is specified in the request, **protected_instance_ids** will be ignored.
limit	No	Integer	Specifies the maximum number of results returned each time. The value is a positive integer from 0 to 1000. The default value is **1000**.

Parameter	Mandatory	Type	Description
offset	No	Integer	Specifies the offset of each request. The default value is **0**. The value must be a positive integer and cannot be negative.
status	No	String	Specifies the status of a protected instance. For details, see **Protected Instance Status**.
name	No	String	Specifies the name of a protected instance. Fuzzy search is supported.
query_type	No	String	Specifies the query type. ● **status_abnormal**: indicates to query protected instances in the abnormal status. ● This parameter is invalid when the value is set to **general** or left empty.
availability_zone	No	String	Specifies the current production site AZ of the protection group containing the protected instance. You can obtain this value by calling the API described in **Querying an Active-Active Domain**.

Request

- Request parameter description

  None

- Example request

```
GET https://{Endpoint}/v1/{project_id}/protected-instances?server_group_ids=%5b
%2221d65fa4-430e-4761-b9ad-4e27364f874c%22%2c%22943c7d15-0371-4b89-b1a6-
db1ef35c9263%22%5d&status=available
```

  NOTE

  Use URL encoding for **server_group_ids** or **protected_instance_ids**.

Response

- Parameter description

Parameter	Type	Description
protected_instances	Array of objects	Specifies the information about protected instances. For details, see **Table 5-18**.
count	Integer	Specifies the number of protected instances.

Table 5-18 protected_instances field description

Parameter	Type	Description
id	String	Specifies the ID of a protected instance.
name	String	Specifies the name of a protected instance.
description	String	Specifies the description of a protected instance.
server_group_id	String	Specifies the ID of a protection group.
status	String	Specifies the status of a protected instance. For details, see **Protected Instance Status**.
progress	Integer	Specifies the synchronization progress of a protected instance. Unit: %
source_server	String	Specifies the production site server ID.
target_server	String	Specifies the DR site server ID.
created_at	String	Specifies the time when a protected instance was created. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.
updated_at	String	Specifies the time when a protected instance was updated. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.

Parameter	Type	Description
priority_station	String	Specifies the current production site AZ of the protection group containing the protected instance. ● **source**: indicates that the current production site AZ is the **source_availability_zone** value. ● **target**: indicates that the current production site AZ is the **target_availability_zone** value.
attachment	Array of objects	Specifies the attached replication pairs. For details, see **Table 5-19**.
tags	Array of objects	Specifies the tag list. For details, see **Table 5-20**.
metadata	Object	Specifies the metadata of a protected instance. For details, see **Table 5-21**.

Table 5-19 attachment field description

Parameter	Type	Description
replication	String	Specifies the ID of a replication pair.
device	String	Specifies the device name.

Table 5-20 tags field description

Parameter	Type	Description
key	String	Specifies the tag key.
value	String	Specifies the tag value.

Table 5-21 Field **metadata** description

Parameter	Type	Description
__system__frozen	String	Specifies whether the resource is frozen. ● **true**: indicates that the resource is frozen. ● Empty: indicates that the resource is not frozen.

- Example response

```
{
    "protected_instances": [
        {
            "id": "67a2cc7e-fb87-41a8-ba28-9c032abcaee1",
            "name": "protected_instance_xff",
            "description": "protected_instance_xff",
            "server_group_id": "21d65fa4-430e-4761-b9ad-4e27364f874c",
            "status": "available",
            "progress": 0,
            "source_server": "d1e8e8a7-ae6f-4f40-bead-20093976961e",
            "target_server": "9bad52b9-ca5a-4274-ba9e-3c8ca9843fa1",
            "created_at": "2018-11-06 11:09:25.861",
            "updated_at": "2018-11-06 11:12:11.716",
            "priority_station": "source",
            "attachment": [
                {
                    "replication": "08d6b5a0-9a12-4263-a468-30d71d10498c",
                    "device": "/dev/vdb"
                },
                {
                    "replication": "4c332757-dc77-458d-9883-03d701cde2f2",
                    "device": "/dev/vda"
                }
            ],
            "tags": [
                {
                   "key": "aaaaaaa",
                   "value": "01234567889"
                 },
                {
                    "key": "ffffff",
                    "value": "dddd"
                }
            ],
            "metadata": {}
        },
        {
            "id": "50f5091e-9e9e-473c-a932-2a2cbcbeb1ff",
            "name": "ecs_sdrs_test",
            "description": "1111",
            "server_group_id": "943c7d15-0371-4b89-b1a6-db1ef35c9263",
            "status": "protected",
            "progress": 100,
            "source_server": "5fb92d6c-b0cb-46c9-824b-b90ec5500ae6",
            "target_server": "c6c0ff54-fa1f-43ef-9ccc-1774e40c8745",
            "created_at": "2018-11-06 09:27:52.258",
            "updated_at": "2018-11-06 09:44:59.853",
            "priority_station": "target",
            "attachment": [
                {
                    "replication": "6568f7c4-0510-4f39-929d-8ffccbd4fd47",
                    "device": "/dev/vda"
                }
            ],
            "tags": [
                {
                    "key": "aaaaaaa",
                    "value": "01234567889"
                },
                {
                    "key": "ffffff",
                    "value": "dddd"                }
            ],
            "metadata": {}
        }
    ],
    "count": 2
}
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not 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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.5.4 Querying Details About a Protected Instance

Function

This API is used to query the details about a protected instance, such as the protected instance ID and name.

Constraints and Limitations

None

URI

- URI format

  GET /v1/{project_id}/protected-instances/{protected_instance_id}

- Parameter description

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

Parameter	Mandatory	Type	Description
protected_instance_id	Yes	String	Specifies the ID of a protected instance. You can obtain this value by calling the API described in **Querying Protected Instances**.

Request

- Request parameters

  None

- Example request

  GET https://{Endpoint}/v1/{project_id}/protected-instances/50f5091e-9e9e-473c-a932-2a2cbcbeb1ff

Response

- Parameter description

Parameter	Type	Description
protected_instance	Object	Specifies the details about a protected instance. For details, see **Table 5-22**.

Table 5-22 protected_instances field description

Parameter	Type	Description
id	String	Specifies the ID of a protected instance.
name	String	Specifies the name of a protected instance.
description	String	Specifies the description of a protected instance.
server_group_id	String	Specifies the ID of a protection group.
status	String	Specifies the status of a protected instance. For details, see **Protected Instance Status**.
progress	Integer	Specifies the synchronization progress of a protected instance. Unit: %

Parameter	Type	Description
source_server	String	Specifies the production site server ID.
target_server	String	Specifies the DR site server ID.
created_at	String	Specifies the time when a protected instance was created. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.
updated_at	String	Specifies the time when a protected instance was updated. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.
priority_station	String	Specifies the current production site AZ of the protection group containing the protected instance. ● **source**: indicates that the current production site AZ is the **source_availability_zone** value. ● **target**: indicates that the current production site AZ is the **target_availability_zone** value.
attachment	Array of objects	Specifies the attached replication pairs. For details, see **Table 5-19**.
tags	Array of objects	Specifies the tag list. For details, see **Table 5-20**.
metadata	Object	Specifies the metadata of a protected instance. For details, see **Table 5-21**.

Table 5-23 attachment field description

Parameter	Type	Description
replication	String	Specifies the ID of a replication pair.
device	String	Specifies the device name.

Table 5-24 tags field description

Parameter	Type	Description
key	String	Specifies the tag key.
value	String	Specifies the tag value.

Table 5-25 Field **metadata** description

Parameter	Type	Description
__system__frozen	String	Specifies whether the resource is frozen. ● **true**: indicates that the resource is frozen. ● Empty: indicates that the resource is not frozen.

- Example response

```
{
    "protected_instance": {
        "id": "50f5091e-9e9e-473c-a932-2a2cbcbeb1ff",
        "name": "ecs_sdrs_test",
        "description": "1111",
        "server_group_id": "943c7d15-0371-4b89-b1a6-db1ef35c9263",
        "status": "available",
        "progress": 0,
        "source_server": "5fb92d6c-b0cb-46c9-824b-b90ec5500ae6",
        "target_server": "c6c0ff54-fa1f-43ef-9ccc-1774e40c8745",
        "created_at": "2018-11-06 09:27:52.258",
        "updated_at": "2018-11-06 09:44:59.853",
        "priority_station": "target",
        "attachment": [
            {
                "replication": "6568f7c4-0510-4f39-929d-8ffccbd4fd47",
                "device": "/dev/vda"
            }
        ],
        "tags": [
            {
                "key": "aaaaaaa",
                "value": "01234567889"
             },
             {
                "key": "ffffff",
                "value": "dddd"
              }
            ],
         "metadata": {}
    }
}
```

Or

```
{
     "error": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.

Returned Value	Description
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.5.5 Changing the Name of a Protected Instance

Function

This API is used to change the name of a protected instance.

Constraints and Limitations

None

URI

- URI format

  PUT /v1/{project_id}/protected-instances/{protected_instance_id}

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
protected_instance_id	Yes	String	Specifies the ID of a protected instance. You can obtain this value by calling the API described in **Querying Protected Instances**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
protected_instance	Yes	Object	Specifies the information about a protected instance. For details, see **Table 5-26**.

Table 5-26 protected_instance field description

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the name of a protected instance. The name can contain a maximum of 64 bytes. The value can contain only letters (a to z and A to Z), digits (0 to 9), decimal points (.), underscores (_), and hyphens (-).

- Example request

  PUT https://{Endpoint}/v1/{project_id}/protected-instances/00000000632302f501632305f63c000e

```
{
    "protected_instance": {
        "name": "test_protected_instance_name"
    }
 }
```

Response

- Parameter description

Parameter	Type	Description
protected_instance	Object	Specifies the details about a protected instance. For details, see **Table 5-27**.

Table 5-27 protected_instance field description

Parameter	Type	Description
id	String	Specifies the ID of a protected instance.
name	String	Specifies the name of a protected instance. The name can contain a maximum of 64 bytes consisting of only letters (a to z and A to Z), digits (0 to 9), decimal points (.), underscores (_), and hyphens (-).
description	String	Specifies the description of a protected instance.
server_group_id	String	Specifies the ID of a protection group.
status	String	Specifies the status of a protected instance. For details, see **Protected Instance Status**.

Parameter	Type	Description
progress	Integer	Specifies the synchronization progress of a protected instance. Unit: %
source_server	String	Specifies the production site server ID.
target_server	String	Specifies the DR site server ID.
created_at	String	Specifies the time when a protected instance was created. The default format is as follows: "yyyy-MM-dd HH:mm:ss.S", for example, **2019-04-01 12:00:00.0**.
updated_at	String	Specifies the time when a protected instance was updated. The default format is as follows: "yyyy-MM-dd HH:mm:ss.S", for example, **2019-04-01 12:00:00.0**.
priority_station	String	Specifies the current production site AZ of the protection group containing the protected instance. ● **source**: indicates that the current production site AZ is the **source_availability_zone** value. ● **target**: indicates that the current production site AZ is the **target_availability_zone** value.
attachment	Array of objects	Specifies the attached replication pairs. For details, see **Table 5-28**.
tags	Array of objects	Specifies the tag list. For details, see **Table 5-29**.
metadata	Object	Specifies the metadata of a protected instance. For details, see **Table 5-30**.

Table 5-28 attachment field description

Parameter	Type	Description
replication	String	Specifies the ID of a replication pair.
device	String	Specifies the device name.

Table 5-29 tags field description

Parameter	Type	Description
key	String	Specifies the tag key.
value	String	Specifies the tag value.

Table 5-30 metadata field description

Parameter	Type	Description
__system__frozen	String	Specifies whether the resource is frozen. ● **true**: indicates that the resource is frozen. ● Empty: indicates that the resource is not frozen.

- Example response

```
{
    "protected_instance": {
      "id": "00000000632302f501632305f63c000e",
      "name": "test_protected_instance_name",
      "description": "_sdrs_protected_instance",
      "server_group_id": "00000000632302f501632305ac75000a",
      "status": "available",
      "progress": 0,
      "source_server": "5597a320-7a36-4462-9f85-a0d01edfb416",
      "target_server": "e37ed7de-bd76-4189-8445-be747205322d",
      "created_at": "2018-05-02 22:43:03.0",
      "updated_at": "2018-05-02 22:47:27.0",
      "priority_station": "target",
      "attachment": [
        {
           "replication": "6568f7c4-0510-4f39-929d-8ffccbd4fd47",
           "device": "/dev/vda"
        }
     ],
     "tags": [
        {
           "key": "aaaaaaa",
           "value": "01234567889"
         },
         {
           "key": "ffffff",
           "value": "dddd"
          }
        ],
      "metadata": {}
 }
 }
```

Or

```
{
    "error": {
      "message": "XXXX",
      "code": "XXX"
    }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.

Returned Value	Description
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.5.6 Attaching a Replication Pair to a Protected Instance

Function

This API is used to attach the specified replication pair to the specified protected instance.

Constraints and Limitations

- **status** of the protection group must be **available** or **protected**.
- **status** of the protected instance must be **available** or **protected**.
- **status** of the replication pair must be **available** or **protected**.
- The non-shared replication pair has not been attached to any protected instance.

URI

- URI format

  POST /v1/{project_id}/protected-instances/{protected_instance_id}/attachreplication

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
protected_instance_id	Yes	String	Specifies the ID of a protected instance. You can obtain this value by calling the API described in **Querying Protected Instances**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
replicationAttachment	Yes	Object	Attaches a replication pair to a protected instance. For details, see **Table 5-31**.

Table 5-31 replicationAttachment field description

Parameter	Mandatory	Type	Description
replication_id	Yes	String	Specifies the ID of a replication pair. You can obtain this value by calling the API described in **Querying Replication Pairs**.
device	Yes	String	Specifies the disk device name of a replication pair. **NOTE** ● The new disk device name cannot be the same as an existing one. ● Set the parameter value to **/dev/sda** for the system disks of protected instances created using Xen servers and to **/dev/sd***x* for data disks, where *x* is a letter in alphabetical order. For example, if there are two data disks, set the device names of the two data disks to **/dev/sdb** and **/dev/sdc**, respectively. If you set a device name starting with **/dev/vd**, the system uses **/dev/sd** by default. ● Set the parameter value to **/dev/vda** for the system disks of protected instances created using KVM servers and to **/dev/vd***x* for data disks, where *x* is a letter in alphabetical order. For example, if there are two data disks, set the device names of the two data disks to **/dev/vdb** and **/dev/vdc**, respectively. If you set a device name starting with **/dev/sd**, the system uses **/dev/vd** by default.

- Example request

  POST https://{Endpoint}/v1/{project_id}/protected-instances/00000000632302f501632305f63c000e/attachreplication

```
{
    "replicationAttachment": {
       "replication_id": "6568f7c4-0510-4f39-929d-8ffccbd4fd47",
       "device": "/dev/vda"
    }
 }
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the job ID. This is a returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
   "job_id": "0000000062db92d70162db9d200f00bb"
 }
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.

Returned Value	Description
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.5.7 Detaching a Replication Pair from a Protected Instance

Function

This API is used to detach a specified replication pair from a specified protected instance.

Constraints and Limitations

- **status** of the protection group must be **available**, **protected**, **failed-over**, **error-starting**, **error-stopping**, **error-reversing**, or **error-failing-over**.
- **status** of the protected instance must be **available**, **protected**, **failed-over**, **error-starting**, **error-stopping**, **error-reversing**, **error-failing-over**, **error-deleting**, **error-reprotecting**, **error-resizing**, **invalid**, or **fault**.
- **status** of the replication pair must be **available**, **protected**, **failed-over**, **error-attaching**, **error-detaching**, **error-starting**, **error-stopping**, **error-**

reversing, **error-failing-over**, **error-deleting**, **error-reprotecting**, **error-extending**, **invalid**, or **fault**.

- The replication pair has been attached to a protected instance.

NOTE

- A system disk (attached to **/dev/sda** or **/dev/vda**) can be detached only when the server is in the **Stopped** state. Therefore, stop the server before detaching the system disk.
- Data disks can be detached online or offline, which means that the server containing the disks can either be in the **Running** or **Stopped** state.

  For details about how to detach a disk online, see **Disk** > **Detaching an EVS Disk from a Running ECS** in the *Elastic Cloud Server User Guide*.

URI

- URI format

  DELETE /v1/{project_id}/protected-instances/{protected_instance_id}/detachreplication/{replication_id}

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
protected_instance_id	Yes	String	Specifies the ID of a protected instance. You can obtain this value by calling the API described in **Querying Protected Instances**.
replication_id	Yes	String	Specifies the ID of a replication pair. You can query replication pairs attached to the protected instance by calling the API described in **Querying Replication Pairs**.

Request

- Request parameters

  None

- Example request

  DELETE http://{Endpoint}/v1/{project_id}/protected-instances/00000000632302f501632305f63c000e/detachreplication/6568f7c4-0510-4f39-929d-8ffccbd4fd47

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the job ID. This is a returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
  "job_id": "0000000062db92d70162db921dgf00bb"
}
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not find the requested page.

Returned Value	Description
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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.5.8 Adding an NIC to a Protected Instance

Function

This API is used to add an NIC to the specified protected instance.

Constraints and Limitations

- **status** of the protection group must be **available** or **protected**.
- **status** of the protected instance must be **available** or **protected**.
- The subnet of the NIC to be added must belong to the same VPC of the protected group and protected instance.

URI

- URI format

  POST /v1/{project_id}/protected-instances/{protected_instance_id}/nic
- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
protected_instance_id	Yes	String	Specifies the ID of a protected instance. You can obtain this value by calling the API described in **Querying Protected Instances**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
subnet_id	Yes	String	Specifies the subnet ID of the NIC to be added. It is **network_id** of the subnet, which is the same as the **neutron_network_id** value.
security_groups	No	Array of objects	Specifies the security group of the NIC to be added. Specifies the security group of the NIC. For details, see **Table 5-32**.
ip_address	No	String	Specifies an IP address. If this parameter is not included, an IP address is automatically assigned.

Table 5-32 security_groups field description

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the ID of a security group.

- Example request

POST https://{Endpoint}/v1/{project_id}/protected-instances/00000000632302f501632305f63c000e/nic

```
{

        "subnet_id": "d32019d3-bc6e-4319-9c1d-6722fc136a23",
        "security_groups": [
          {
                "id": "f0ac4394-7e4a-4409-9701-ba8be283dbc3"
            }
        ],
        "ip_address": "192.168.97.25",

}
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the job ID. This is a returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
  "job_id": "0000000062db92d70162db9d200f32dh"
 }
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.

Returned Value	Description
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.5.9 Deleting an NIC from a Protected Instance

Function

This API is used to delete an NIC from the specified protected instance.

Constraints and Limitations

- **status** of the protection group must be **available** or **protected**.
- **status** of the protected instance must be **available** or **protected**.
- The primary NIC cannot be deleted.

URI

- URI format

POST /v1/{project_id}/protected-instances/{protected_instance_id}/nic/delete

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
protected_instance_id	Yes	String	Specifies the ID of a protected instance. You can obtain this value by calling the API described in **Querying Protected Instances**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
nic_id	Yes	String	Specifies the port ID of the NIC.

- Example request

POST https://{Endpoint}/v1/{project_id}/protected-instances/00000000632302f501632305f63c000e/nic/delete

```
{
    "nic_id": "f0ac4394-7e4a-4409-9701-husge283dbc3"
}
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the job ID. This is a returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
  "job_id": "0000000011db92d70162db9d20df32ch"
}
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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.

Returned Value	Description
502 Bad Gateway	Failed to complete the request because the server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.5.10 Modifying the Specifications of a Protected Instance

Function

This API is used to modify the specifications of a server in a protected instance, including:

- Modify the specifications of both the production and DR site servers.
- Modify the specifications of only the production site server.
- Modify the specifications of only the DR site server.

You can perform this operation only when the servers of which the specifications to be modified are stopped.

NOTE

Servers of different specifications have different performance, which may affect applications running on the servers. To ensure the server performance after a planned failover or failover, you are recommended to use servers of specifications (CPU and memory) same or higher than the specifications of the production site servers at the DR site.

Constraints and Limitations

- **status** of the protection group must be **available** or **protected**.
- **status** of the protected instance must be **available**, **protected**, or **error-resizing**.
- Servers of which the specifications to be modified are stopped.

URI

- URI format

  POST /v1/{project_id}/protected-instances/{protected_instance_id}/resize
- Parameter description

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

Parameter	Mandatory	Type	Description
protected_instance_id	Yes	String	Specifies the ID of a protected instance. You can obtain this value by calling the API described in **Querying Protected Instances**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
resize	Yes	Object	Modifies the specifications of a protected instance. For details, see **Table 5-33**.

Table 5-33 **resize** field description

Parameter	Mandatory	Type	Description
flavorRef	No	String	Specifies the flavor ID of the production and DR site servers after the modification. **NOTE** If you specify this parameter, the system modifies the specifications of both the production and DR site servers. After the modification, the production site server and DR site server use the same specifications.
production_flavorRef	No	String	Specifies the flavor ID of the production site server after the modification. **NOTE** • If you specify this parameter, the system modifies the specifications of only the production site server. • If **flavorRef** is specified, **production_flavorRef** does not take effect.

Parameter	Mandatory	Type	Description
dr_flavorRef	No	String	Specifies the flavor ID of the DR site server after the modification. **NOTE** ● If you specify this parameter, the system modifies the specifications of only the DR site server. ● If **flavorRef** is specified, **dr_flavorRef** does not take effect.
production_dedicated_host_id	No	String	Specifies the new DeH ID for the production site. **NOTE** ● If the production site server is created on a DeH, this parameter must be specified when you modify the specifications of the production site server. ● You can set this parameter to the ID of the DeH where the production site server is currently located or the ID of another DeH.
dr_dedicated_host_id	No	String	Specifies the new DeH ID for the DR site. **NOTE** ● If the DR site server is created on a DeH, this parameter must be specified when you modify the specifications of the DR site server. ● You can set this parameter to the ID of the DeH where the DR site server is currently located or the ID of another DeH.

- Example request

  POST https://{Endpoint}/v1/{project_id}/protected-instances/00000000632302f501632305f63c000e/resize

  Example 1: Modify the specifications of the production and DR site servers to e2.small. Example request:

```
{
     "resize": {
         "flavorRef": "e2.small"
      }
 }
```

  Example 2: Modify the specifications of the production and DR site serves to s3.small.1 and s3.large.2 respectively. Example request:

```
{
     "resize": {
        "production_flavorRef": "s3.small.1",
        "dr_flavorRef": "s3.large.2"
    }
}
```

Example 3: Modify the specifications of the production site server to e2.small, and retain the DR site server specifications. Example request:

```
{
    "resize": {
        "production_flavorRef": "e2.small"
    }
}
```

Example 4: Modify the specifications of the DR site server to e2.small, and retain the production site server specifications. Example request:

```
{
    "resize": {
        "dr_flavorRef": "e2.small"
    }
}
```

Example 5: The production site server is created on a DeH. Modify the specifications of the production site server to e2.small, and retain the DR site server specifications. The following lists the example request.

```
{
    "resize": {
        "production_flavorRef": "e2.small",
        "production_dedicated_host_id": "59f82ad6-6fc9-4bae-8621-aef2194e112c"
    }
}
```

Example 6: The DR site server is created on a DeH. Modify the specifications of the DR site server to e2.small, and retain the production site server specifications. The following lists the example request.

```
{
    "resize": {
        "dr_flavorRef": "e2.small",
        "dr_dedicated_host_id": "59f82ad6-6fc9-4bae-8621-aef2194e112c"
    }
}
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the job ID. This is a returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
  "job_id": "0000000011db92d70162db9d20df32ch"
}
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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.

Returned Value	Description
502 Bad Gateway	Failed to complete the request because the server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.5.11 Batch Creating Protected Instances

Function

This API is used to batch create protected instances. When a protected instance is created, the default name of the server at the DR site is the same as that of the server at the production site, but their IDs are different. To modify a server name, click the server name on the protected instance details page to switch to the server details page and modify the server name. Alternatively, you can call the API in **Changing the Name of a Protected Instance** to modify the name.

Constraints and Limitations

- **status** of the protection group must be **available** or **protected**.
- If you want to use a server with a shared disk attached to create a protected instance, ensure that all the servers with the shared disk attached are in the creation list if you want to create the protected instances in batches.
- No protected instance has been created using the server.
- The server must be in the same VPC as the protection group.
- If protection is enabled for servers created during capacity expansion of an AS group, these servers cannot be deleted when the capacity of the AS group is reduced.
- If the server at the production site runs Windows and you choose the key login mode, ensure that the key pair of the server exists when you create a protected instance. Otherwise, the server at the DR site may fail to create, causing the protected instance creation failure.

  NOTE

  If the key pair of the production site server has been deleted, create a key pair with the same name.
- If the production site server is added to Enterprise Project, the created DR site server will not be automatically added to Enterprise Project. You need to manually add it to Enterprise Project if needed.
- After you create a protected instance and enable protection on servers at the production site, modifications to the **Hostname**, **Name**, **Security Group**, **Agency**, **ECS Group**, **Tags**, and **Auto Recovery** configurations of servers on the production site will not synchronize to the servers at the DR site. You can manually add the configuration items to the servers at the DR site on the management console.

URI

- URI format

  POST /v1/{project_id}/protected-instances/batch

- Parameter description

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

Request

- Parameter description

Parameter	Mandatory	Type	Description
protected_instances	Yes	Object	Specifies the information about a protected instance. For details, see **Table 5-34**.

Table 5-34 protected_instances field description

Parameter	Mandatory	Type	Description
name_prefix	Yes	String	Specifies the prefix of a protected instance name. When you create protected instances in batches, the system will automatically add a suffix to each protected instance name prefix to differentiate the protected instances, such as "-0001". Each protected instance name prefix can contain 1 to 59 characters, and consists of only letters (a to z and A to Z), digits (0 to 9), decimal points (.), underscores (_), and hyphens (-).

Parameter	Mandatory	Type	Description
description	No	String	Specifies the description of protected instances. The description can contain a maximum of 64 characters. The value cannot contain the left angle bracket (<) or right angle bracket (>).
server_group_id	Yes	String	Specifies the ID of the protection group where the protected instances are added. For details, see **Querying Protection Groups**.
cluster_id	No	String	Specifies the DSS storage pool ID. This parameter needs to be specified if the DR site disk uses DSS.
primary_subnet_id	No	String	Specifies the subnet ID of the primary NIC on the DR site server. The value is the same as that of **neutron_network_id**.
servers	Yes	Array of objects	Specifies the servers for creating protected instances. For details, see **Table 5-35**. **NOTE** A maximum of five servers are supported by default.
tenancy	No	String	Specifies whether the DR site server is created on a DeH or in a shared pool. The value can be **shared** or **dedicated**. **shared**: indicates the shared pool. **dedicated**: indicates the DeH.
dedicated_host_id	No	String	Specifies the DeH ID. This parameter takes effect only when **tenancy** is set to **dedicated**. If you do not specify this parameter, the system will automatically assign a DeH to a tenant to deploy servers.

Parameter	Mandatory	Type	Description
tags	No	Array of objects	Specifies the tag list. For details, see **Table 5-36**. **NOTE** ● The tags will be added to each protected instance created in this batch. ● A maximum of 10 tags can be added in this list.

Table 5-35 Data structure of the **server_info** field

Parameter	Mandatory	Type	Description
server_id	Yes	String	Specifies the ID of the production site server. **NOTE** When the API is successfully invoked, the DR site server will be automatically created.
flavorRef	No	String	Specifies the flavor ID of the DR site server. **NOTE** ● If this parameter is not specified, the flavor ID of the DR site server is the same as that of the production site server by default. ● Servers of different specifications have different performance, which may affect applications running on the servers. To ensure the server performance after a planned failover or failover, you are recommended to use servers of specifications (CPU and memory) same or higher than the specifications of the production site servers at the DR site.

Table 5-36 resource_tag field description

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. The tag key of a resource must be unique. It can contain up to 36 Unicode characters. The tag key cannot be left blank or be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), equal signs (=), commas (,), vertical bars (|), and slashes (/). The key cannot be left blank, and must be unique for each resource.
value	Yes	String	Specifies the tag value. It can contain up to 43 Unicode characters. The value cannot be left blank but can be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), equal signs (=), commas (,), vertical bars (|), and slashes (/).

- Example request

  POST https://{Endpoint}/v1/{project_id}/protected-instances/batch

```
{
        "protected_instances":{
              "name_prefix": "test_protected_instance_name",
              "description": "my description",
              "server_group_id": "523ab8ad-3759-4933-9436-4cf4ebb20867",
              "primary_subnet_id": "a32217fh-3413-c313-6342-3124d3491502",
              "servers": [
                 {
                     "server_id": "403b603d-1d91-42cc-a357-81f3c2daf43f",
                     "flavorRef":"c3.medium.2"
                 },
                 {
                      "server_id": "8f5dd226-6cc0-4fe8-9786-b8b3359b234b"
                 }
              ],
              "tenancy": "dedicated",
              "dedicated_host_id": "0bc41598-1b5a-4bd2-872a-82e6abb82e68",
              "tags": [
                 {
                     "key": "test",
                     "value":"aaaaa"
                 }
              ],
    }
}
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	This is a returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
  "job_id": "0000000062db92d70162db9d200f00bb"
 }
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

Returned Value

- Normal

Returned Value	Description
202	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not find the requested page.

Returned Value	Description
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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.5.12 Batch Deleting Protected Instances

Function

This API is used to batch delete protected instances.

Constraints and Limitations

- **status** of the protected instance must be **available**, **protected**, **failed-over**, **error**, **error-starting**, **error-stopping**, **error-reversing**, **error-failing-over**, **error-deleting**, **error-reprotecting**, **error-resizing**, **invalid**, or **fault**.
- Protected instances are from the same protection group.
- If a shared replication pair is attached to multiple protected instances, ensure that all the protected instances with the shared replication pair attached are in the deletion list if you want to delete them in batches.

URI

- URI format

  POST /v1/{project_id}/protected-instances/delete

- Parameter description

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

Request

- Parameter description

Parameter	Mandatory	Type	Description
protected_instances	Yes	Array of objects	Specifies the protected instances to be deleted. For details, see **Table 5-37**. **NOTE** • A maximum of 20 protected instances are supported by default.
delete_target_server	No	Boolean	Specifies whether to delete the DR site server. The default value is **false**.
delete_target_eip	No	Boolean	Specifies whether to delete the EIP of the DR site server. The default value is **false**.

Table 5-37 Data structure of the **protected_instance** field

Parameter	Mandatory	Type	Description
id	Yes	String	Specifies the ID of a protected instance. For details, see **Querying Protected Instances**.

- Example request

POST https://{Endpoint}/v1/{project_id}/protected-instances/delete

```
{
   "protected_instances": [
              {
                 "id": "127842d5-f98e-451e-963e-9fb464fbb911"
```

```
            },
            {
                "id": "8f5dd226-6cc0-4fe8-9786-b8b3359b234b"
            }
          ],
  "delete_target_server": false,
  "delete_target_eip": false
}
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	This is a returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
  "job_id": "0000000062db92d70162db3ab00f00df"
 }
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

Returned Value

- Normal

Returned Value	Description
202	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.

Returned Value	Description
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.6 Replication Pair

5.6.1 Creating a Replication Pair

Function

This API is used to create a replication pair and add it to the specified protection group.

Constraints and Limitations

- **status** of the protection group must be **available** or **protected**.
- If **server_type** of the protection group is set to **ECS**, the disk status is **Available**.

URI

- URI format

  POST /v1/{project_id}/replications

- Parameter description

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

Request

- Parameter description

Parameter	Mandatory	Type	Description
replication	Yes	Object	Specifies the information about a replication pair. For details, see **Table 5-38**.

Table 5-38 replication field description

Parameter	Mandatory	Type	Description
server_group_id	Yes	String	Specifies the ID of a protection group. You can obtain this value by calling the API described in **Querying Protection Groups**.
volume_id	Yes	String	Specifies the ID of the production site disk. **NOTE** When the API is successfully invoked, the DR site disk will be automatically created.
name	Yes	String	Specifies the name of a replication pair. The name can contain a maximum of 64 bytes. The value can contain only letters (a to z and A to Z), digits (0 to 9), decimal points (.), underscores (_), and hyphens (-).

Parameter	Mandatory	Type	Description
description	No	String	Specifies the description of a replication pair. The value can contain a maximum of 64 bytes and cannot contain the left angle bracket (<) or right angle bracket (>).
cluster_id	No	String	Specifies the DSS storage pool ID.

- Example request

  POST https://{Endpoint}/v1/{project_id}/replications

```
{
   "replication": {
      "server_group_id": "c79fba33-b165-4c69-80c1-d7e590691162",
      "volume_id": "b6f71149-7b9c-4f36-8ff0-1c4809a6f2c2",
      "name": "replication_name",
      "description": "replication_description"
  }
 }
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the job ID. This is a returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
  "job_id": "0000000011db92d36662db9d20df32ch"
 }
```

  Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

  In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.6.2 Deleting a Replication Pair

Function

This API is used to delete a specified replication pair.

Constraints and Limitations

- **status** of the protection group must be **available**, **protected**, **failed-over**, **error-starting**, **error-stopping**, **error-reversing**, or **error-failing-over**, **error-deleting**, or **error-reprotecting**.
- **status** of the replication pair must be **available**, **protected**, **failed-over**, **error**, **error-starting**, **error-stopping**, **error-reversing**, **error-failing-over**, **error-deleting**, **error-reprotecting**, **error-attaching**, **error-extending**, **invalid**, or **fault**.
- The replication pair has not been attached to a protected instance.

URI

- URI format

  DELETE /v1/{project_id}/replications/{replication_id}
- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
replication_id	Yes	String	Specifies the ID of a replication pair. You can obtain this value by calling the API described in **Querying Replication Pairs**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
replication	Yes	Object	Specifies the information about a replication pair. For details, see **Table 5-39**.

Table 5-39 replication field description

Parameter	Mandatory	Type	Description
server_group_id	No	String	Specifies the ID of a protection group.
delete_target_volume	No	Boolean	Specifies whether to delete the DR site disk. The default value is **false**.

- Example request

  DELETE https://{Endpoint}/v1/{project_id}/replications/b93bc1c4-67ee-45a1-bc8a-d022fdd28811

```
{
  "replication": {
      "server_group_id": "c79fba33-b165-4c69-80c1-d7e590691162",
       "delete_target_volume": false
  }
}
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the job ID. This is a returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
  "job_id": "0000000011db92d34587db9d20df32ch"
}
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.6.3 Querying Replication Pairs

Function

This API is used to query all replication pairs in a specified protection group. If you do not specify the protection group, the system lists all the replication pairs of the tenant.

Constraints and Limitations

None

URI

- URI format

  GET /v1/{project_id}/replications

- Parameter description

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

- **Request filter** field description

Parameter	Mandatory	Type	Description
server_group_id	No	String	Specifies the ID of a protection group. You can obtain this value by calling the API described in **Querying Protection Groups**.

Parameter	Mandatory	Type	Description
server_group_ids	No	Array of strings	Specifies the protection group ID list. The value is in the following format: server_group_ids=['server_group_id1','server_group_id2',...,'server_group_idx']. Convert it using URL encoding. - All the replication pairs with valid **server_group_id** in **server_group_ids** are returned. - The replication pairs of a maximum of 30 **server_group_id** values can be queried. - If parameters **server_group_id** and **server_group_ids** are both specified in the request, **server_group_id** will be ignored.
protected_instance_id	No	String	Specifies the ID of a protected instance. You can obtain this value by calling the API described in **Querying Protected Instances**.
protected_instance_ids	No	Array of strings	Specifies the protected instance ID list. The value is in the following format: protected_instance_ids=['protected_instance_id1','protected_instance_id2',...,'protected_instance_idx']. Convert it using URL encoding. - All the replication pairs with valid **protected_instance_id** in **protected_instance_ids** are returned. - The replication pairs of a maximum of 30 **protected_instance_id** values can be queried. - If parameters **protected_instance_id** and **protected_instance_ids** are both specified in the request, **protected_instance_id** will be ignored.
name	No	String	Specifies the name of a replication pair. Fuzzy search is supported.

Parameter	Mandatory	Type	Description
status	No	String	Specifies the status of a replication pair. For details, see **Replication Pair Status**.
limit	No	Integer	Specifies the maximum number of results returned each time. The value is a positive integer from 0 to 1000. The default value is **1000**.
offset	No	Integer	Specifies the offset of each request. The default value is **0**. The value must be a number and cannot be negative.
query_type	No	String	Specifies the query type. ● To query replication pairs in the abnormal status, set **query_type** to **status_abnormal**. ● Otherwise, set **query_type** to general or leave it empty.
availability_zone	No	String	Specifies the current production site AZ of the protection group containing the replication pair. You can obtain this value by calling the API described in **Querying an Active-Active Domain**.
volume_id	No	String	Specifies the ID of the disk used to create a replication pair.

Request

- Request parameters

  None

- Example request

```
https://{Endpoint}/v1/{project_id}/replications?server_group_ids=%5b%2221d65fa4-430e-4761-
b9ad-4e27364f874c%22%2c%22943c7d15-0371-4b89-b1a6-db1ef35c9263&status=available
```

NOTE

Use URL encoding for **server_group_ids** or **protected_instance_ids**.

Response

- Parameter description

Parameter	Type	Description
replications	Array of objects	Specifies the information about replication pairs. For details, see **Table 5-40**.
count	Integer	Specifies the number of replication pairs.

Table 5-40 replications field description

Parameter	Type	Description
id	String	Specifies the ID of a replication pair.
name	String	Specifies the name of a replication pair.
description	String	Specifies the description of a replication pair.
replication_model	String	Specifies the replication mode of a replication pair. The default value is **hypermetro**, indicating synchronous replication.
status	String	Specifies the status of a replication pair. For details, see **Replication Pair Status**.
progress	Integer	Specifies the synchronization progress of a replication pair. Unit: %
replication_status	String	Specifies the data synchronization status. ● **active**: Data has been synchronized. ● **inactive**: Data is not synchronized. ● **copying**: Data is being synchronized. ● **active-stopped**: Data synchronization is stopped.
attachment	Array of objects	Specifies the device name. For details, see **Table 5-41**.
server_group_id	String	Specifies the ID of a protection group.
volume_ids	String	Specifies the ID of the disk used to create a replication pair.

Parameter	Type	Description
priority_station	String	Specifies the current production site AZ of the protection group containing the replication pair. ● **source**: indicates that the current production site AZ is the **source_availability_zone** value. ● **target**: indicates that the current production site AZ is the **target_availability_zone** value.
fault_level	String	Specifies the fault level of a replication pair. ● **0**: No fault occurs. ● **2**: The disk of the current production site does not have read/write permissions. In this case, you are advised to perform a failover. ● **5**: The replication link is disconnected. In this case, a failover is not allowed. Contact customer service.
created_at	String	Specifies the time when a replication pair was created. The default format is as follows: ""yyyy-MM-ddTHH:mm:ss.SSSSSS", for example, **2019-04-01T12:00:00.000000**.
updated_at	String	Specifies the time when a replication pair was updated. The default format is as follows: ""yyyy-MM-ddTHH:mm:ss.SSSSSS", for example, **2019-04-01T12:00:00.000000**.
record_metadata	Object	Specifies the SDR data of a replication pair. For details, see **Table 5-42**.
failure_detail	String	Specifies the error code returned only when **status** of a replication pair is **error**. For details, see the returned value in **Error Codes**.

Table 5-41 attachment field description

Parameter	Type	Description
device	String	Specifies the device name.
protected_instance	String	Specifies the ID of the protected instance to which the replication pair is attached.

Table 5-42 record_metadata field description

Parameter	Type	Description
multiattach	Boolean	Specifies whether the disk in a replication pair is a shared disk.
bootable	Boolean	Specifies whether the disk in a replication pair is a system disk.
volume_size	Integer	Specifies the size of the disk in a replication pair. Unit: GB
volume_type	String	Specifies the type of the disk in a replication pair. The value can be **SSD**, **GPSSD**, or **SAS**. ● **SSD**: the ultra-high I/O type ● **GPSSD**: the general purpose SSD type ● **SAS**: the high I/O type

- Example response

```
{
    "count": 1,
    "replications": [
        {
            "id": "b93bc1c4-67ee-45a1-bc8a-d022fdd28811",
            "name": "test_replication_name",
            "description": "description_test",
            "replication_model": "hypermetro",
            "status": "available",
            "progress": 0,
            "replication_status": "active",
            "attachment": [
                {
                    "device": "/dev/vda",
                    "protected_instance": "8a7a6339-679b-452b-948c-144e0ef85d9e"
                }
            ],
            "server_group_id": "c2aee29a-2959-4d01-9755-01cc76a4d17d",
            "volume_ids": "48dda0c0-c800-46f2-9728-a519ff783d35,388b324a-a9d1-44a4-
a00d-42085f22a9bc",
            "priority_station": "source",
            "fault_level": "0",
            "created_at": "2018-05-04T03:43:24.108526",
            "updated_at": "2018-05-04T03:44:28.322873",
            "record_metadata": {
                "multiattach": false,
                "bootable": false,
                "volume_size": 10,
                "volume_type": "SATA"
            }
        }
    ]
}
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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.

Returned Value	Description
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.6.4 Querying Details About a Replication Pair

Function

This API is used to query the details about a replication pair.

Constraints and Limitations

None

URI

- URI format

  GET /v1/{project_id}/replications/{replication_id}

- 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**.
replication_id	Yes	Specifies the ID of a replication pair. You can obtain this value by calling the API described in **Querying Replication Pairs**.

Request

- Request parameters

  None

- Example request

  GET https://{Endpoint}/v1/{project_id}/replications/b93bc1c4-67ee-45a1-bc8a-d022fdd28811

Response

- Parameter description

Parameter	Type	Description
replication	Object	Specifies the information about a replication pair. For details, see **Table 5-43**.

Table 5-43 replication field description

Parameter	Type	Description
id	String	Specifies the ID of a replication pair.
name	String	Specifies the name of a replication pair.
description	String	Specifies the description of a replication pair.
replication_model	String	Specifies the replication mode of a replication pair. The default value is **hypermetro**, indicating synchronous replication.
status	String	Specifies the status of a replication pair. For details, see **Replication Pair Status**.
progress	Integer	Specifies the synchronization progress of a replication pair. Unit: %
replication_status	String	Specifies the data synchronization status. ● **active**: Data has been synchronized. ● **inactive**: Data is not synchronized. ● **copying**: Data is being synchronized. ● **active-stopped**: Data synchronization is stopped.

Parameter	Type	Description
attachment	Array of objects	Specifies the device name. For details, see **Table 5-44**.
server_group_id	String	Specifies the ID of a protection group.
volume_ids	String	Specifies the ID of the disk used to create a replication pair.
priority_station	String	Specifies the current production site AZ of the protection group containing the replication pair. ● **source**: indicates that the current production site AZ is the **source_availability_zone** value. ● **target**: indicates that the current production site AZ is the **target_availability_zone** value.
fault_level	String	Specifies the fault level of a replication pair. ● **0**: No fault occurs. ● **2**: The disk of the current production site does not have read/write permissions. In this case, you are advised to perform a failover. ● **5**: The replication link is disconnected. In this case, a failover is not allowed. Contact customer service.
created_at	String	Specifies the time when a replication pair was created. The default format is as follows: ""yyyy-MM-ddTHH:mm:ss.SSSSSS", for example, **2019-04-01T12:00:00.000000**.
updated_at	String	Specifies the time when a replication pair was updated. The default format is as follows: ""yyyy-MM-ddTHH:mm:ss.SSSSSS", for example, **2019-04-01T12:00:00.000000**.
record_metadata	Object	Specifies the SDR data of a replication pair. For details, see **Table 5-45**.

Parameter	Type	Description
failure_detail	String	Specifies the error code returned only when **status** of a replication pair is **error**. For details, see the returned value in **Error Codes**.

Table 5-44 attachment field description

Parameter	Type	Description
device	String	Specifies the device name.
protected_instance	String	Specifies the ID of the protected instance to which the replication pair is attached.

Table 5-45 record_metadata field description

Parameter	Type	Description
multiattach	Boolean	Specifies whether the disk in a replication pair is a shared disk.
bootable	Boolean	Specifies whether the disk in a replication pair is a system disk.
volume_size	Integer	Specifies the size of the disk in a replication pair. Unit: GB
volume_type	String	Specifies the type of the disk in a replication pair. The value can be **SSD**, **GPSSD**, or **SAS**. ● **SSD**: the ultra-high I/O type ● **GPSSD**: the general purpose SSD type ● **SAS**: the high I/O type

- Example response

```
{
    "replication":
        {
            "id": "b93bc1c4-67ee-45a1-bc8a-d022fdd28811",
            "name": "test_sdrs_replication",
            "description": "test_description",
            "replication_model": "hypermetro",
            "status": "available",
            "progress": 0,
            "replication_status": "active",
            "attachment": [
                {
                    "device": "/dev/vda",
                    "protected_instance": "8a7a6339-679b-452b-948c-144e0ef85d9c"
                }
            ],
            "server_group_id": "c2aee29a-2959-4d01-9755-01cc76a4d17d",
            "volume_ids": "48dda0c0-c800-46f2-9728-a519ff783d35,388b324a-a9d1-44a4-
a00d-42085f22a9bc",
            "priority_station": "source",
            "fault_level": "0",
            "created_at": "2018-05-04T03:43:24.108526",
            "updated_at": "2018-05-04T03:44:28.322873",
            "record_metadata": {
                "multiattach": false,
                "bootable": false,
                "volume_size": 10,
                "volume_type": "SATA"
            }
        }
}
```

Or

```
{
     "error": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
     "badrequest": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not find the requested page.
405 Method Not Allowed	You are not allowed to use the method specified in the request.

Returned Value	Description
406 Not Acceptable	The response generated by the server could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.6.5 Expanding the Capacity of a Replication Pair

Function

This API is used to expand the capacity of the two disks in a replication pair.

Constraints and Limitations

- **status** of the replication pair must be **available**, **protected**, or **error-extending**.
- **status** of disks in the replication pair is **available** or **in-use**.
- If the billing mode of the disks in the replication pair is yearly/monthly, capacity expansion is not supported. If you want to increase the capacity of disks in the replication pair, delete the replication pair, expand the capacity of the production site disk, and then use the disk to create a replication pair.

NOTE

- When the disks in a replication pair are not shared

  Capacity expansion is supported even if the disks in the replication pair are in the **in-use** state.
- When the disks in a replication pair are shared

  The replication pair capacity cannot be expanded online if the disks are in the **in-use** state.

URI

- URI format

  POST /v1/{project_id}/replications/{replication_id}/action

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
replication_id	Yes	String	Specifies the ID of a replication pair. You can obtain this value by calling the API described in **Querying Replication Pairs**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
extend-replication	Yes	Object	Expands disk capacity. For details, see **Table 5-46**.

Table 5-46 extend-replication field description

Parameter	Mandatory	Type	Description
new_size	Yes	Integer	Specifies the disk capacity after expansion in a replication pair. Unit: GB **NOTE** If the value has a decimal point, the system takes the integer before the decimal point by default.

- Example request

  POST https://{Endpoint}/v1/{project_id}/replications/b93bc1c4-67ee-45a1-bc8a-d022fdd28811/action

```
{
    "extend-replication": {
        "new_size": 10
    }
}
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the job ID. This is a returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
  "job_id": "0000000011db92d34587db9d20df32ch"
}
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not find the requested page.

Returned Value	Description
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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.6.6 Changing the Name of a Replication Pair

Function

This API is used to change the name of a replication pair.

Constraints and Limitations

None

URI

- URI format

  PUT /v1/{project_id}/replications/{replication_id}

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
replication_id	Yes	String	Specifies the ID of a replication pair. You can obtain this value by calling the API described in **Querying Replication Pairs**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
replication	Yes	Object	Specifies the information about a replication pair. For details, see **Table 5-47**.

Table 5-47 replication field description

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the name of a replication pair. ● The name can contain a maximum of 64 bytes. ● The value can contain only letters (a to z and A to Z), digits (0 to 9), decimal points (.), underscores (_), and hyphens (-).

- Example request

  PUT https://{Endpoint}/v1/{project_id}/replications/b93bc1c4-67ee-45a1-bc8a-d022fdd28811

```
{
    "replication": {
        "name": "new_name"
    }
}
```

Response

- Parameter description

Parameter	Type	Description
replication	Object	Specifies the information about a replication pair. For details, see **Table 5-48**.

Table 5-48 replication field description

Parameter	Type	Description
id	String	Specifies the ID of a replication pair.
name	String	Specifies the name of a replication pair. The name can contain a maximum of 64 bytes consisting of only letters (a to z and A to Z), digits (0 to 9), decimal points (.), underscores (_), and hyphens (-).
description	String	Specifies the description of a replication pair.
replication_model	String	Specifies the replication mode of a replication pair. The default value is **hypermetro**, indicating synchronous replication.
status	String	Specifies the status of a replication pair. For details, see **Replication Pair Status**.
progress	Integer	Specifies the synchronization progress of a replication pair. Unit: %
replication_status	String	Specifies the data synchronization status. ● **active**: Data has been synchronized. ● **inactive**: Data is not synchronized. ● **copying**: Data is being synchronized. ● **active-stopped**: Data synchronization is stopped.
attachment	Array of objects	Specifies the device name. For details, see **Table 5-49**.

Parameter	Type	Description
volume_ids	String	Specifies the ID of the disk used to create a replication pair.
server_group_id	String	Specifies the ID of a protection group.
priority_station	String	Specifies the current production site AZ of the protection group containing the replication pair. ● **source**: indicates that the current production site AZ is the **source_availability_zone** value. ● **target**: indicates that the current production site AZ is the **target_availability_zone** value.
fault_level	String	Specifies the fault level of a replication pair. ● **0**: No fault occurs. ● **2**: The disk of the current production site does not have read/write permissions. In this case, you are advised to perform a failover. ● **5**: The replication link is disconnected. In this case, a failover is not allowed. Contact customer service.
created_at	String	Specifies the time when a replication pair was created. The default format is as follows: ""yyyy-MM-ddTHH:mm:ss.SSSSSS", for example, **2019-04-01T12:00:00.000000**.
updated_at	String	Specifies the time when a replication pair was updated. The default format is as follows: "yyyy-MM-ddTHH:mm:ss.SSSSSS", for example, **2019-04-01T12:00:00.000000**.
record_metadata	Object	Specifies the SDR data of a replication pair. For details, see **Table 5-50**.
failure_detail	String	Specifies the error code returned only when **status** of a replication pair is **error**. For details, see the returned value in **Error Codes**.

Table 5-49 attachment field description

Parameter	Type	Description
protected_instance	String	Specifies the ID of the protected instance to which the replication pair is attached.
device	String	Specifies the device name.

Table 5-50 record_metadata field description

Parameter	Type	Description
multiattach	Boolean	Specifies whether the disk in a replication pair is a shared disk.
bootable	Boolean	Specifies whether the disk in a replication pair is a system disk.
volume_size	Integer	Specifies the size of the disk in a replication pair. Unit: GB
volume_type	String	Specifies the type of the disk in a replication pair. The value can be **SSD**, **GPSSD**, or **SAS**. ● **SSD**: the ultra-high I/O type ● **GPSSD**: the general purpose SSD type ● **SAS**: the high I/O type

- Example response

```
{
    "replication":
        {
            "id": "b93bc1c4-67ee-45a1-bc8a-d022fdd28811",
            "name": "new_name",
            "description": "test_description",
            "replication_model": "hypermetro",
            "status": "available",
            "progress": 0,
            "replication_status": "active",
            "attachment": [
                {
                    "device": "/dev/vda",
                    "protected_instance": "8a7a6339-679b-452b-948c-144e0ef85d9c"
                }
            ],
            "volume_ids": "48dda0c0-c800-46f2-9728-a519ff783d35,388b324a-a9d1-44a4-
a00d-42085f22a9bc",
            "server_group_id": "0000000062d194520162d196f0fe0007",
            "priority_station": "source",
            "fault_level": "0",
            "created_at": "2018-05-04T03:43:24.108526",
            "updated_at": "2018-05-04T03:44:28.322873",
            "record_metadata": {
                "multiattach": false,
                "bootable": false,
                "volume_size": "10",
                "volume_type": "SATA"
            }
        }
}
```

Or

```
{
    "error": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
}
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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.

Returned Value	Description
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.7 DR Drill

5.7.1 Creating a DR Drill

Function

This API is used to create a disaster recovery (DR) drill.

Constraints and Limitations

- **status** of the protection group must be **available**, **protected**, **failed-over**, **error-starting**, **error-stopping**, **error-reversing**, **error-reprotecting**, or **error-failing-over**.
- Do not perform a DR drill before the first time data synchronization completes. Otherwise, the drill server may not start properly.
- If the DR site server of the protection group is added to Enterprise Project, the created DR drill server will not be automatically added to Enterprise Project. You need to manually add it to Enterprise Project if needed.
- If **drill_vpc_id** is specified (the system uses an existing drill VPC), the drill VPC CIDR block must be consistent with that of the VPC for the protection group. If **drill_vpc_id** is not specified, the system automatically creates a drill VPC.
- When you use a created drill VPC to create a drill, the subnet ACL rule of the drill VPC will be different from that of the VPC of the protection group. You need to manually set them to be the same one if needed.
- When you create a DR drill, if the VPC of the protection group has a customized routing table and subnets configured, the corresponding routing table will not be automatically created for the drill VPC. You need to manually create it if needed.

URI

- URI format

  POST /v1/{project_id}/disaster-recovery-drills
- Parameter description

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

Request

- Parameter description

Parameter	Mandatory	Type	Description
disaster_recovery_drill	Yes	Object	Specifies the information about a DR drill. For details, see **Table 5-51**.

Table 5-51 disaster_recovery_drill field description

Parameter	Mandatory	Type	Description
server_group_id	Yes	String	Specifies the ID of a protection group. For details, see **Querying Protection Groups**.
drill_vpc_id	No	String	Specifies the drill VPC ID. If you do not specify this parameter, the system will automatically create a drill VPC.
name	Yes	String	Specifies the name of a DR drill. The name can contain a maximum of 64 bytes. The value can contain only letters (a to z and A to Z), digits (0 to 9), decimal points (.), underscores (_), and hyphens (-).

- Example request

  POST https://{Endpoint}/v1/{project_id}/disaster-recovery-drills

```
{
        "disaster_recovery_drill": {
                "name": "dr_drill_test",
                "server_group_id":"c2aee29a-2959-4d01-9755-01cc76a4d17d",
                "drill_vpc_id":"87d505be-e984-455e-ad84-588c73fb258b"
    }
}
```

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the job ID. This is a returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
    "job_id": "0000000011db92d36662db9d20df32ch"
 }
```

Or

```
{
      "error": {
          "message": "XXXX",
          "code": "XXX"
      }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
      "badrequest": {
          "message": "XXXX",
          "code": "XXX"
      }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.

Returned Value	Description
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.7.2 Deleting a DR Drill

Function

This API is used to delete a specified DR drill. After you delete the specified DR drill:

- The DR drill as well as the disks and NICs attached to the DR drill will be deleted.
- The drill VPC and subnets of the drill VPC will not be deleted. You can create other servers using this VPC.

Constraints and Limitations

The status of the DR drill must be **available**, **error**, or **error-deleting**.

URI

- URI format

  DELETE /v1/{project_id}/disaster-recovery-drills/{disaster_recovery_drill_id}

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
disaster_recovery_drill_id	Yes	String	Specifies the DR drill ID. To query details, see **Querying DR Drills**.

Request

- Request parameters

  None

- Example request

  DELETE https://{Endpoint}/v1/{project_id}/disaster-recovery-drills/f96ac55f-35dd-4cc3-ba61-36c168900c99

Response

- Parameter description

Parameter	Type	Description
job_id	String	Specifies the job ID. This is a returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.

- Example response

```
{
   "job_id": "0000000011db92d34587db9d20df32ch"
 }
```

Or

```
{
     "error": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
        "message": "XXXX",
        "code": "XXX"
    }
 }
```

Returned Value

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.

Returned Value	Description
504 Gateway Timeout	A gateway timeout error occurred.

5.7.3 Querying DR Drills

Function

This API is used to query all DR drills in a specified protection group. If you do not specify the protection group, the system lists all the DR drills of the tenant.

Constraints and Limitations

None

URI

- URI format

  GET /v1/{project_id}/disaster-recovery-drills

- Parameter description

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

- **Request filter** field description

Parameter	Mandatory	Type	Description
server_group_id	No	String	Specifies the ID of a protection group. For details, see **Querying Protection Groups**.
name	No	String	Specifies the DR drill name. Fuzzy search is supported.
status	No	String	Specifies the DR drill status. For details, see **DR Drill Status**.
drill_vpc_id	No	String	Specifies the ID of the VPC used for a DR drill.

Parameter	Mandatory	Type	Description
limit	No	Integer	Specifies the maximum number of results returned each time. The value is a positive integer from 0 to 1000. The default value is **1000**.
offset	No	Integer	Specifies the offset of each request. The default value is **0**. The value must be a number and cannot be negative.

Request

- Request parameters

  None
- Example request

  GET https://{Endpoint}/v1/{project_id}/disaster-recovery-drills

Response

- Parameter description

Parameter	Type	Description
disaster_recovery_drills	Array of objects	Specifies the DR drills. For details, see **Table 5-52**.
count	Integer	Specifies the number of DR drills.

Table 5-52 disaster_recovery_drills field description

Parameter	Type	Description
id	String	Specifies the DR drill ID.
name	String	Specifies the DR drill name.
status	String	Specifies the DR drill status. For details, see **DR Drill Status**.
server_group_id	String	Specifies the ID of a protection group.
drill_vpc_id	String	Specifies the ID of the VPC used for a DR drill.

Parameter	Type	Description
created_at	String	Specifies the time when a DR drill was created. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.
updated_at	String	Specifies the time when a DR drill was updated. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.
drill_servers	Array of objects	Specifies the drill servers. For details, see **Table 5-53**.

Table 5-53 drill_servers field description

Parameter	Type	Description
protected_instance	String	Specifies the protected instance ID of the drill server.
drill_server_id	String	Specifies the drill server ID.

- Example response

```
{
    "count": 2,
    "disaster_recovery_drills": [
      {
          "id": "e472d26f-9624-42fb-8bfc-717d4714c225",
          "name": "dr_drill_test",
          "status": "available",
          "server_group_id": "c2aee29a-2959-4d01-9755-01cc76a4d17d",
          "drill_vpc_id": "7881f1d2-1f41-419c-873a-14ac620bc46e",
          "created_at": "2018-07-18 06:41:58.681",
          "updated_at": "2018-07-18 09:41:14.677",
          "drill_servers": [
              {
                  "protected_instance": "d08ca8d7-a784-41ae-b32a-c592943f5dfc",
                  "drill_server_id": "9de0439a-4ee4-4199-919a-44afd20952dc"
              },
              {
                  "protected_instance": "ea308e8b-043c-4fc6-a53c-856eae137b13",
                  "drill_server_id": "3eaa1c70-9719-4eb5-b577-cb92ddbffd03"
              }
          ]
      },
      {
          "id": "f96ac55f-35dd-4cc3-ba61-36c168900c99",
          "name": "drill_test",
          "status": "available",
          "server_group_id": "3a60f45d-cf5b-49f1-a05e-ddee78cb6eef",
          "drill_vpc_id": "ac784bd6-a79c-4def-9ff8-dc87940d5335",
          "created_at": "2018-07-17 22:38:21.111",
          "updated_at": "2018-07-17 22:47:54.845",
          "drill_servers": []
```

```
        }
    ]
}
```

Or

```
{
     "error": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
     "badrequest": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

Returned Value

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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.

Returned Value	Description
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.7.4 Querying Details About a DR Drill

Function

This API is used to query the details about a DR drill.

Constraints and Limitations

None

URI

- URI format

  GET /v1/{project_id}/disaster-recovery-drills/{disaster_recovery_drill_id}

- 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**.
disaster_recovery_drill_id	Yes	Specifies the DR drill ID. To query details, see **Querying DR Drills**.

Request

- Request parameters

  None

- Example request

  GET https://{Endpoint}/v1/{project_id}/disaster-recovery-drills/e472d26f-9624-42fb-8bfc-717d4714c225

Response

- Parameter description

Parameter	Type	Description
disaster_recovery_drill	Object	Specifies the information about a DR drill. For details, see **Table 5-54**.

Table 5-54 disaster_recovery_drill field description

Parameter	Type	Description
id	String	Specifies the DR drill ID.
name	String	Specifies the DR drill name.
status	String	Specifies the DR drill status. For details, see **DR Drill Status**.
drill_vpc_id	String	Specifies the ID of the VPC used for a DR drill.
created_at	String	Specifies the time when a DR drill was created. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.
updated_at	String	Specifies the time when a DR drill was updated. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.
server_group_id	String	Specifies the ID of a protection group.
drill_servers	Array of objects	Specifies the drill servers. For details, see **Table 5-55**.

Table 5-55 drill_servers field description

Parameter	Type	Description
protected_instance	String	Specifies the protected instance ID of the drill server.
drill_server_id	String	Specifies the drill server ID.

- Example response

```
{
    "disaster_recovery_drill":
        {
          "id": "e472d26f-9624-42fb-8bfc-717d4714c225",
          "name": "dr_drill_test",
          "status": "available",
          "server_group_id": "c2aee29a-2959-4d01-9755-01cc76a4d17d",
          "drill_vpc_id": "7881f1d2-1f41-419c-873a-14ac620bc46e",
          "created_at": "2018-07-18 06:41:58.681",
          "updated_at": "2018-07-18 00:41:14.677",
          "drill_servers": [
              {
                  "protected_instance": "d08ca8d7-a784-41ae-b32a-c592943f5dfc",
                  "drill_server_id": "9de0439a-4ee4-4199-919a-44afd20952dc"
              },
              {
                  "protected_instance": "ea308e8b-043c-4fc6-a53c-856eae137b13",
                  "drill_server_id": "3eaa1c70-9719-4eb5-b577-cb92ddbffd03"
              }
          ]
        }
 }
```

Or

```
{
     "error": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
     "badrequest": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

Returned Value

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not find the requested page.
405 Method Not Allowed	You are not allowed to use the method specified in the request.

Returned Value	Description
406 Not Acceptable	The response generated by the server could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.7.5 Updating a DR Drill Name

Function

This API is used to update a DR drill name.

Constraints and Limitations

None

URI

- URI format

  PUT /v1/{project_id}/disaster-recovery-drills/{disaster_recovery_drill_id}

- Parameter description

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

Parameter	Mandatory	Description
disaster_recovery_drill_id	Yes	Specifies the DR drill ID. To query details, see **Querying DR Drills**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
disaster_recovery_drill	Yes	Object	Specifies the information about a DR drill. For details, see **Table 5-56**.

Table 5-56 disaster_recovery_drill field description

Parameter	Mandatory	Type	Description
name	Yes	String	Specifies the DR drill name. ● The name can contain a maximum of 64 bytes. ● The value can contain only letters (a to z and A to Z), digits (0 to 9), decimal points (.), underscores (_), and hyphens (-).

- Example request

  PUT https://{Endpoint}/v1/{project_id}/disaster-recovery-drills/e472d26f-9624-42fb-8bfc-717d4714c225

```
{
    "disaster_recovery_drill": {
        "name": "new_dr_drill_name"
    }
 }
```

Response

- Parameter description

Parameter	Type	Description
disaster_recovery_drill	Object	Specifies the information about a DR drill. For details, see **Table 5-57**.

Table 5-57 disaster_recovery_drill field description

Parameter	Type	Description
id	String	Specifies the DR drill ID.
name	String	Specifies the DR drill name. Specifies the name of a DR drill. The name can contain a maximum of 64 bytes. The value can contain only letters (a to z and A to Z), digits (0 to 9), decimal points (.), underscores (_), and hyphens (-).
status	String	Specifies the DR drill status. For details, see **DR Drill Status**.
drill_vpc_id	String	Specifies the ID of the VPC used for a DR drill.
created_at	String	Specifies the time when a DR drill was created. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.
updated_at	String	Specifies the time when a DR drill was updated. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.
server_group_id	String	Specifies the ID of a protection group.
drill_servers	Array of objects	Specifies the drill servers. For details, see **Table 5-58**.

Table 5-58 drill_servers field description

Parameter	Type	Description
protected_instance	String	Specifies the protected instance ID of the drill server.

Parameter	Type	Description
drill_server_id	String	Specifies the drill server ID.

- Example response

```
{
    "disaster_recovery_drill":
       {
          "id": "e472d26f-9624-42fb-8bfc-717d4714c225",
         "name": "new_dr_drill_name",
         "status": "available",
         "server_group_id": "c2aee29a-2959-4d01-9755-01cc76a4d17d",
         "drill_vpc_id": "7881f1d2-1f41-419c-873a-14ac620bc46e",
         "created_at": "2018-07-18 06:41:58.681",
         "updated_at": "2018-07-18 00:41:14.677",
         "drill_servers": [
           {
             "protected_instance": "d08ca8d7-a784-41ae-b32a-c592943f5dfc",
             "drill_server_id": "9de0439a-4ee4-4199-919a-44afd20952dc"
           },
           {
             "protected_instance": "ea308e8b-043c-4fc6-a53c-856eae137b13",
             "drill_server_id": "3eaa1c70-9719-4eb5-b577-cb92ddbffd03"
           }
         ]
       }
 }
```

Or

```
{
    "error": {
       "message": "XXXX",
       "code": "XXX"
    }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
    "badrequest": {
       "message": "XXXX",
       "code": "XXX"
    }
 }
```

Returned Value

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.

Returned Value	Description
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.8 Tag Management

5.8.1 Querying Protected Instances by Tag

Function

This API is used to query protected instances by tag.

URI

- URI format

  POST /v1/{project_id}/protected-instances/resource_instances/action
- Parameter description

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

Request

- Parameter description

Parameter	Mandatory	Type	Description
offset	No	String	Specifies the index position. This parameter is unavailable when **action** is set to **count**. If **offset** is set to *N*, the resource query starts from the N+1 piece of data. If **action** is set to **filter**, the value of **offset** is **0** by default, indicating that the query starts from the first piece of data. The **offset** value must be a number and cannot be a negative number.
limit	No	String	Specifies the number of limited queries. This parameter is unavailable when **action** is set to **count**. The default value is **1000** when **action** is set to **filter**. The maximum value is **1000**, and the minimum value is **1**. The value cannot be a negative number.
action	Yes	String	Specifies the operation to be performed. The value can be **filter** (filtering) or **count** (querying the total number). If **action** is set to **filter**, the query is performed based on the filter conditions. If **action** is set to **count**, only the total number of records is returned.

Parameter	Mandatory	Type	Description
matches	No	Array of objects	Specifies the search field. The tag key is the field to be matched, for example, **resource_name**. The tag value indicates the value to be matched. The key is a fixed dictionary value and cannot contain duplicate keys or unsupported keys. Determine whether fuzzy match is required based on the keys. For example, if **key** is **resource_name**, fuzzy search (case insensitive) is used by default. If **value** is an empty string, exact match is used. Currently, only **resource_name** for **key** is supported. Other **key** values will be available later. For details, see **Table 5-60**.
not_tags	No	Array of objects	The resources to be queried do not contain tags listed in **not_tags**. Each resource to be queried contains a maximum of 10 keys. Each tag key can have a maximum of 10 tag values. The tag value corresponding to each tag key can be an empty array but the structure cannot be missing. Each tag key must be unique, and each tag value in a tag must be unique. The response returns resources containing no tags in this list. Keys in this list are in an AND relationship while values in each key-value structure are in an OR relationship. If no tag filtering condition is specified, full data is returned. For details, see **Table 5-59**.

Parameter	Mandatory	Type	Description
tags	No	Array of objects	The resources to be queried contain tags listed in **tags**. Each resource to be queried contains a maximum of 10 keys. Each tag key can have a maximum of 10 tag values. The tag value corresponding to each tag key can be an empty array but the structure cannot be missing. Each tag key must be unique, and each tag value in a tag must be unique. The response returns resources containing all tags in this list. Keys in this list are in an AND relationship while values in each key-value structure are in an OR relationship. If no tag filtering condition is specified, full data is returned. For details, see **Table 5-59**.
tags_any	No	Array of objects	The resources to be queried contain any tags listed in **tags_any**. Each resource to be queried contains a maximum of 10 keys. Each tag key can have a maximum of 10 tag values. The tag value corresponding to each tag key can be an empty array but the structure cannot be missing. Each tag key must be unique, and each tag value in a tag must be unique. The response returns resources containing the tags in this list. Keys in this list are in an OR relationship and values in each key-value structure are also in an OR relationship. If no tag filtering condition is specified, full data is returned. For details, see **Table 5-59**.

Parameter	Mandatory	Type	Description
not_tags_any	No	Array of objects	The resources to be queried do not contain any tags listed in **not_tags_any**. Each resource to be queried contains a maximum of 10 keys. Each tag key can have a maximum of 10 tag values. The tag value corresponding to each tag key can be an empty array but the structure cannot be missing. Each tag key must be unique, and each tag value in a tag must be unique. The response returns resources containing no tags in this list. Keys in this list are in an OR relationship and values in each key-value structure are also in an OR relationship. If no tag filtering condition is specified, full data is returned. For details, see **Table 5-59**.

Table 5-59 tag field description

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. It contains a maximum of 127 Unicode characters. It cannot be left blank. **key** cannot be empty, an empty string, or spaces. Before using **key**, delete spaces of single-byte character (SBC) before and after the value.

Parameter	Mandatory	Type	Description
values	Yes	Array of strings	Lists the tag values. Each value contains a maximum of 255 Unicode characters. Before using **values**, delete SBC spaces before and after the value. The asterisk (*) is reserved for the system. If the value starts with *, it indicates that fuzzy match is performed based on the value following *. The value cannot contain only asterisks (*). If the values are null, it indicates **any_value** (querying any value). The resources containing one or more values listed in **values** will be found and displayed.

Table 5-60 Description of the **match** field

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. Currently, only **resource_name** for **key** is supported. Other **key** values will be available later.
value	Yes	String	Specifies the tag value. Each value can contain a maximum of 255 Unicode characters.

- Sample request when **action** is set to **filter**

  POST https://{Endpoint}/v1/{project_id}/protected-instances/resource_instances/action

```
{
    "offset": "100",
    "limit": "100",
    "action": "filter",
    "matches": [
        {
            "key": "resource_name",
            "value": "resource1"
        }
    ],
    "not_tags": [
        {
            "key": "key1",
            "values": [
                "*value1",
                "value2"
            ]
        }
    ],
    "tags": [
        {
            "key": "key1",
            "values": [
                "*value1",
                "value2"
            ]
        }
    ],
    "tags_any": [
        {
            "key": "key1",
            "values": [
                "value1",
                "value2"
            ]
        }
    ],
    "not_tags_any": [
        {
            "key": "key1",
            "values": [
                "value1",
                "value2"
            ]
        }
    ]
}
```

- Sample request when **action** is set to **count**

  POST https://{Endpoint}/v1/{project_id}/protected-instances/resource_instances/action

```
{
    "action": "count",
    "not_tags": [
        {
            "key": "key1",
            "values": [
                "value1",
                "*value2"
            ]
        }
    ],
    "tags": [
        {
            "key": "key1",
            "values": [
                "value1",
                "value2"
            ]
        },
        {
            "key": "key2",
            "values": [
                "value1",
                "value2"
            ]
        }
    ],
    "tags_any": [
        {
            "key": "key1",
            "values": [
                "value1",
                "value2"
            ]
        }
    ],
    "not_tags_any": [
        {
            "key": "key1",
            "values": [
                "value1",
                "value2"
            ]
        }
    ],
    "matches": [
        {
            "key": "resource_name",
            "value": "resource1"
        }
    ]
}
```

Response

- Parameter description

Parameter	Mandatory	Type	Description
resources	Yes	Array of objects	Specifies the returned protected instances. For details, see **Table 5-61**.
total_count	Yes	Integer	Specifies the total number of resources. The value is not affected by the filtering criteria.

Table 5-61 Description of field **resource**

Parameter	Mandatory	Type	Description
resource_id	Yes	String	Specifies the ID of a protected instance.
resource_name	Yes	String	Specifies the protected instance name. This parameter is left blank by default if there is no name.
resource_detail	Yes	Object	Specifies the details of a protected instance. For details, see **Table 5-62**.

Parameter	Mandatory	Type	Description
tags	Yes	Array of objects	Specifies the tag list. If there is no tag in the list, **tags** is taken as an empty array. For details, see **Table 5-66**.

Table 5-62 protected_instances field description

Parameter	Type	Description
id	String	Specifies the ID of a protected instance.
name	String	Specifies the name of a protected instance.
description	String	Specifies the description of a protected instance.
server_group_id	String	Specifies the ID of a protection group.
status	String	Specifies the status of a protected instance. For details, see **Protected Instance Status**.
progress	Integer	Specifies the synchronization progress of a protected instance. Unit: %
source_server	String	Specifies the production site server ID.
target_server	String	Specifies the DR site server ID.
created_at	String	Specifies the time when a protected instance was created. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.
updated_at	String	Specifies the time when a protected instance was updated. The default format is as follows: "yyyy-MM-dd HH:mm:ss.SSS", for example, **2019-04-01 12:00:00.000**.

Parameter	Type	Description
priority_station	String	Specifies the current production site AZ of the protection group containing the protected instance. ● **source**: indicates that the current production site AZ is the **source_availability_zone** value. ● **target**: indicates that the current production site AZ is the **target_availability_zone** value.
attachment	Array of objects	Specifies the attached replication pairs. For details, see **Table 5-19**.
tags	Array of objects	Specifies the tag list. For details, see **Table 5-20**.
metadata	Object	Specifies the metadata of a protected instance. For details, see **Table 5-21**.

Table 5-63 attachment field description

Parameter	Type	Description
replication	String	Specifies the ID of a replication pair.
device	String	Specifies the device name.

Table 5-64 tags field description

Parameter	Type	Description
key	String	Specifies the tag key.
value	String	Specifies the tag value.

Table 5-65 Field **metadata** description

Parameter	Type	Description
__system__frozen	String	Specifies whether the resource is frozen. - **true**: indicates that the resource is frozen. - Empty: indicates that the resource is not frozen.

Table 5-66 resource_tag field description

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. The tag key of a resource must be unique. It can contain up to 36 Unicode characters. The key cannot be left blank or be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\\), equal signs (=), commas (,), vertical bars (|), and slashes (/). The key cannot be left blank, and must be unique for each resource.
value	Yes	String	Specifies the value. It can contain up to 43 Unicode characters. The value cannot be left blank but can be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\\), equal signs (=), commas (,), vertical bars (|), and slashes (/).

- Example response

  Example response when **action** is set to **filter**

```
{
    "resources": [
        {
            "resource_id": "d5a00c87-6b82-414a-a09e-59c37fff44d0",
            "resource_name": "Protected-Instance-c801",
            "resource_detail": {
                "id": "d5a00c87-6b82-414a-a09e-59c37fff44d0",
                "name": "Protected-Instance-c801",
                "description": null,
                "server_group_id": "525fbd01-d4d1-44fc-b341-6d734bcce245",
                "status": "protected",
                "progress": 100,
                "source_server": "73aff1d7-48d2-494e-a9f1-a7d3ffad31ff",
                "target_server": "0f6bc56b-a3bb-4707-a4fb-ccd4db5fac59",
                "created_at": "2019-05-28 08:17:50.066",
                "updated_at": "2019-05-30 01:40:00.74",
                "priority_station": "source",
                "attachment": [
                    {
                        "replication": "42e2016e-b96e-4f75-aa57-1377a9cb45e4",
                        "device": "/dev/vda"
                    }
                ],
                "tags": [
                    {
                        "key": "GH1111113fffffKdddddd",
                        "value": "aaappppppppddddddd"
                    }
                ],
                "metadata": {}
            },
            "tags": [
                {
                    "key": "GH1111113fffffKdddddd",
                    "value": "aaappppppppddddddd"
                }
            ]
        }
    ],
    "total_count": 1
}
```

- Example response when **action** is set to **count**

```
{
    "total_count": 1000
}
```

Returned Value

- Normal

Returned Value	Description
200	OK

- Abnormal

Returned Value	Description
400	Invalid parameters.
401	Authentication failed.
403	Insufficient permission.

Returned Value	Description
404	The requested resource was not found.
500	Internal service error.

5.8.2 Adding Protected Instance Tags in Batches

Function

This API is used to add protected instance tags for a specified protected instance in batches.

You can add a maximum of 10 tags to a protected instance.

This API is idempotent.

- If there are duplicate keys in the request body when you add tags, an error is reported.
- During tag creation, duplicate keys are not allowed. If a key exists in the database, its value will be overwritten.

URI

- URI format

  POST /v1/{project_id}/protected-instances/{protected_instance_id}/tags/action
- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
protected_instance_id	Yes	String	Specifies the ID of a protected instance. For details, see **Querying Protected Instances**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
action	Yes	String	Identifies the operation. The value can be **create** or **delete**. ● **create**: indicates to create a tag.
tags	Yes	Array of objects	Specifies the tag list. For details, see **Table 5-67**.

Table 5-67 resource_tag field description

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. The tag key of a resource must be unique. It can contain up to 36 Unicode characters. The key cannot be left blank or be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\\), equal signs (=), commas (,), vertical bars (|), and slashes (/). The key cannot be left blank, and must be unique for each resource.
value	Yes	String	Specifies the tag value. It can contain up to 43 Unicode characters. The value cannot be left blank but can be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\\), equal signs (=), commas (,), vertical bars (|), and slashes (/).

- Example request

POST https://{Endpoint}/v1/{project_id}/protected-instances/67a2cc7e-fb87-41a8-ba28-9c032abcaee1/tags/action

```
{
    "action": "create",
    "tags": [
        {
            "key": "key1",
            "value": "value1"
        },
        {
            "key": "key",
            "value": "value3"
        }
    ]
}
```

Response

- Parameter description

  None

Returned Value

- Normal

Returned Value	Description
204	No Content

- Abnormal

Returned Value	Description
400	Invalid parameters.
401	Authentication failed.
403	Insufficient permission.
404	The requested resource was not found.
500	Internal service error.

5.8.3 Deleting Protected Instance Tags in Batches

Function

This API is used to delete protected instance tags for a specified protected instance in batches.

You can add a maximum of 10 tags to a protected instance.

This API is idempotent.

- During tag deletion, if some tags do not exist, the operation is considered to be successful by default. The character set of the tags will not be checked. When you delete tags, the tag structure cannot be missing, and the key cannot be left blank or be an empty string.

URI

- URI format
  POST /v1/{project_id}/protected-instances/{protected_instance_id}/tags/action
- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
protected_instance_id	Yes	String	Specifies the ID of a protected instance. For details, see **Querying Protected Instances**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
action	Yes	String	Identifies the operation. The value can be **create** or **delete**. ● **delete**: indicates to delete a tag.
tags	Yes	Array of objects	Specifies the tag list. For details, see **Table 5-68**.

Table 5-68 resource_tag field description

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. The tag key of a resource must be unique. It can contain up to 36 Unicode characters. The key cannot be left blank or be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\\), equal signs (=), commas (,), vertical bars (|), and slashes (/). The key cannot be left blank, and must be unique for each resource.
value	No	String	Specifies the tag value. The value contains a maximum of 43 Unicode characters. If **value** is specified, tags are deleted by key and value. If **value** is not specified, tags are deleted by key. The value cannot be left blank but can be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\\), equal signs (=), commas (,), vertical bars (|), and slashes (/).

- Example request

  POST https://{Endpoint}/v1/{project_id}/protected-instances/67a2cc7e-fb87-41a8-ba28-9c032abcaee1/tags/action

```
{
    "action": "delete",
    "tags": [
        {
            "key": "key1"
        },
        {
            "key": "key2",
            "value": "value3"
        }
    ]
}
```

Response

- Parameter description

  None

Returned Values

- Normal

Returned Value	Description
204	No Content

- Abnormal

Returned Value	Description
400	Invalid parameters.
401	Authentication failed.
403	Insufficient permission.
404	The requested resource was not found.
500	Internal service error.

5.8.4 Adding a Protected Instance Tag

Function

You can add a maximum of 10 tags to a protected instance.

This API is idempotent.

If a to-be-created tag has the same key as an existing tag, the tag will be created and overwrite the existing one.

URI

- URI format
  POST /v1/{project_id}/protected-instances/{protected_instance_id}/tags
- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
protected_instance_id	Yes	String	Specifies the ID of a protected instance. For details, see **Querying Protected Instances**.

Request

- Parameter description

Parameter	Mandatory	Type	Description
tag	Yes	Object	Specifies the tag to be added. For details, see **Table 5-69**.

Table 5-69 tag field description

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. The tag key of a resource must be unique. It can contain up to 36 Unicode characters. The key cannot be left blank or be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), equal signs (=), commas (,), vertical bars (|), and slashes (/). The key cannot be left blank, and must be unique for each resource.
value	Yes	String	Specifies the tag value. It can contain up to 43 Unicode characters. The value cannot be left blank but can be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), equal signs (=), commas (,), vertical bars (|), and slashes (/).

- Example request

  POST https://{Endpoint}/v1/{project_id}/protected-instances/67a2cc7e-fb87-41a8-ba28-9c032abcaee1/tags

```
{
    "tag": {
        "key": "DEV",
        "value": "DEV1"
    }
}
```

Response

- Example response

  None

Returned Value

- Normal

Returned Value	Description
204	No Content

- Abnormal

Returned Value	Description
400	Invalid parameters.
401	Authentication failed.
403	Insufficient permission.
404	The requested resource was not found.
500	Internal service error.

5.8.5 Deleting a Protected Instance Tag

Function

This API is idempotent.

- During deletion, the tag character set is not verified. The URI must be encoded before the API is invoked. Other services need to decode the URI.

  NOTE

  Select a desired tool for URI encoding.

- The tag key cannot be left blank or be an empty string. If the key of the tag to be deleted does not exist, 404 will be returned.

URI

- URI format

  DELETE /v1/{project_id}/protected-instances/{protected_instance_id}/tags/{key}

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
protected_instance_id	Yes	String	Specifies the ID of a protected instance. For details, see **Querying Protected Instances**.
key	Yes	String	Specifies the tag key.

Request

- Request parameters

  None

- Example request

  DELETE https://{Endpoint}/v1/{project_id}/protected-instances/67a2cc7e-fb87-41a8-ba28-9c032abcaee1/tags/DEV

Response

- Response parameter

  None

- Example response

  None

Returned Value

- Normal

Returned Value	Description
204	No Content

- Abnormal

Returned Value	Description
400	Invalid parameters.
401	Authentication failed.
403	Insufficient permission.
404	The requested resource was not found.
500	Internal service error.

5.8.6 Querying a Protected Instance Tag

Function

This API is used to query tags of a specified protected instance.

URI

- URI format

  GET /v1/{project_id}/protected-instances/{protected_instance_id}/tags

- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
protected_instance_id	Yes	String	Specifies the ID of a protected instance. For details, see **Querying Protected Instances**.

Request

- Request parameters

  None

- Example request

  GET https://{Endpoint}/v1/{project_id}/protected-instances/50f5091e-9e9e-473c-a932-2a2cbcbeb1ff/tags

Response

- Parameter description

Parameter	Mandatory	Type	Description
tags	Yes	Array of objects	Specifies the tag list. For details, see **Table 5-70**.

Table 5-70 resource_tag field description

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. The tag key of a resource must be unique. It can contain up to 36 Unicode characters. The key cannot be left blank or be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), equal signs (=), commas (,), vertical bars (|), and slashes (/). The key cannot be left blank, and must be unique for each resource.
value	Yes	String	Specifies the tag value. It can contain up to 43 Unicode characters. The value cannot be left blank but can be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\), equal signs (=), commas (,), vertical bars (|), and slashes (/).

- Example response

```
{
    "tags": [
        {
            "key": "key1",
            "value": "value1"
        },
        {
            "key": "key2",
            "value": "value3"
        }
    ]
}
```

Returned Value

- Normal

Returned Value	Description
200	OK

- Abnormal

Returned Value	Description
400	Invalid parameters.
401	Authentication failed.
403	Insufficient permission.
404	The requested resource was not found.
500	Internal service error.

5.8.7 Querying Tags of All Protected Instances in a Specified Project

Function

This API is used to query all resource tags of a protected instance in a specified project.

URI

- URI format

  GET /v1/{project_id}/protected-instances/tags

- Parameter description

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

Request

- Request parameters

  None

- Example request

  GET https://{Endpoint}/v1/{project_id}/protected-instances/tags

Response

- Parameter description

Parameter	Mandatory	Type	Description
tags	Yes	Array of objects	Specifies the tag list. For details, see **Table 5-71**.

Table 5-71 Data structure of the **tag** field

Parameter	Mandatory	Type	Description
key	Yes	String	Specifies the tag key. The tag key of a resource must be unique. It can contain up to 36 Unicode characters. The key cannot be left blank or be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\\), equal signs (=), commas (,), vertical bars (|), and slashes (/). The key cannot be left blank, and must be unique for each resource.
values	Yes	Array of strings	Lists the tag values. It can contain up to 43 Unicode characters. The value cannot be left blank but can be an empty string. It cannot contain non-printable ASCII characters (0–31) or special characters, including asterisks (*), left angle brackets (<), right angle brackets (>), backslashes (\\), equal signs (=), commas (,), vertical bars (|), and slashes (/).

- Example response

```
{
    "tags": [
        {
            "key": "key1",
            "values": [
                "value1",
                "value2"
            ]
        },
        {
            "key": "key2",
            "values": [
                "value1",
                "value2"
            ]
        }
    ]
}
```

Returned Value

- Normal

Returned Value	Description
200	OK

- Abnormal

Returned Value	Description
400	Invalid parameters.
401	Authentication failed.
403	Insufficient permission.
404	The requested resource was not found.
500	Internal service error.

5.9 Task Center

You can use the APIs described in this section to query failed tasks of the protection group level, and the failed tasks in a protection group.

5.9.1 Querying Failed Tasks

Function

This API is used to query failed tasks of all protection groups or failed tasks in a specified protection group.

Constraints and Limitations

None

URI

- URI format

  GET /v1/{project_id}/task-center/failure-jobs
- Parameter description

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

- **Request filter** field description

Parameter	Mandatory	Type	Description
failure_status	No	String	Query the task failure status. ● **createFail**: indicates a creation failure. ● **deleteFail**: indicates a deletion failure. ● **attachFail**: indicates an attachment failure. ● **detachFail**: indicates a detachment failure. ● **expandFail**: indicates an expansion failure. ● **resizeFail**: indicates a specification change failure. ● **startFail**: indicates a protection enabling failure. ● **stopFail**: indicates a protection disabling failure. ● **reverseFail**: indicates a planned failover failure. ● **failoverFail**: indicates a failover failure. ● **reprotectFail**: indicates a re-protection enabling failure.
resource_name	No	String	Specifies the resource name of a protection group.
server_group_id	No	String	Specifies the ID of a protection group. For details, see **Querying Protection Groups**.

Parameter	Mandatory	Type	Description
resource_type	No	String	Specifies the resource type. - **server_groups**: indicates a protection group. - **protected_instances**: indicates a protected instance. - **replications**: indicates a replication pair. - **disaster_recovery_drills**: indicates a DR drill.
limit	No	Integer	Specifies the maximum number of results returned each time. The value is a positive integer ranging from **0** to **1000**, and is **1000** by default.
offset	No	Integer	Specifies the offset of each request. The default value is **0**. The value must be a number and cannot be negative.

Request

- Request parameters

  None

- Example request

  GET https://{Endpoint}/v1/{project_id}/task-center/failure-jobs

  GET https://{Endpoint}/v1/{project_id}/task-center/failure-jobs?server_group_id=XXXXX

  NOTE

  - If you do not specify **filter** in the request, the system displays failed tasks of the protection group level, such as failed protection group creation or deletion tasks.
  - To query failed tasks in a protection group, specify **server_group_id** in **filter**.

Response

- Parameter description

Parameter	Type	Description
failure_jobs	list	Specifies the list of the failed tasks. For details, see **Table 5-72**.
count	Integer	Specifies the number of failed tasks in the list.

Table 5-72 failure_jobs field description

Parameter	Type	Description
job_status	String	Specifies the task status. The value can be **FAIL** only in current version. - **FAIL**: The task failed.
resource_id	String	Specifies the resource ID.
resource_name	String	Specifies the resource name.
resource_type	String	Specifies the resource type. - **server_groups**: indicates a protection group. - **protected_instances**: indicates a protected instance. - **replications**: indicates a replication pair. - **disaster_recovery_drills**: indicates a DR drill.
failure_status	String	Specifies the failed task status. - **createFail**: indicates a creation failure. - **deleteFail**: indicates a deletion failure. - **attachFail**: indicates an attachment failure. - **detachFail**: indicates a detachment failure. - **expandFail**: indicates an expansion failure. - **resizeFail**: indicates a specification change failure. - **startFail**: indicates a protection enabling failure. - **stopFail**: indicates a protection disabling failure. - **reverseFail**: indicates a planned failover failure. - **failoverFail**: indicates a failover failure. - **reprotectFail**: indicates a re-protection enabling failure.

Parameter	Type	Description
job_id	String	Specifies the task ID. This is a returned parameter when the asynchronous API command is issued successfully. For details about the task execution result, see the description in **Querying the Job Status**.
job_type	String	Specifies the task name.
begin_time	String	Specifies the task operation time. The default format is as follows: "yyyy-MM-ddTHH:mm:ss.SSSZ", for example, **2019-04-01T12:00:00.000Z**.
error_code	String	Specifies the error code for a failed task.
fail_reason	String	Specifies the task failure cause.

- Example response

```
{
    "count": 2,
    "failure_jobs": [
        {
            "job_status": "FAIL",
            "resource_id": "17984002-ad8a-438b-8ba6-b850224634c5",
            "resource_name": "Protected-Instance-ab14",
            "resource_type": "protectedInstance",
            "failure_status": "createFail",
            "job_id": "ff808082686f229a0168707beaab014e",
            "job_type": "createProtectedInstance",
            "begin_time": "2019-01-21T12:56:35.754Z",
            "error_code": "EVS.2024",
            "fail_reason": "SdrsGenerateNativeServerParamsTask-fail:volume is error!"
        },
        {
            "job_status": "FAIL",
            "resource_id": "897f57b2-6e94-4179-b414-9532726c59f2",
            "resource_name": "Protected-Instance-5e2e",
            "resource_type": "protectedInstance",
            "failure_status": "createFail",
            "job_id": "ff808082686f229a0168707b9be9013e",
            "job_type": "createProtectedInstance",
            "begin_time": "2019-01-21T12:56:15.591Z",
            "error_code": "EVS.2024",
            "fail_reason": "SdrsGenerateNativeServerParamsTask-fail:volume is error!"
        }
    ]
}
```

Or

```
{
     "error": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
     "badrequest": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

Returned Value

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.

Returned Value	Description
504 Gateway Timeout	A gateway timeout error occurred.

5.9.2 Deleting a Failed Task

Function

This API is used to delete a failed task.

Constraints and Limitations

None

URI

- URI format

  DELETE /v1/{project_id}/task-center/failure-jobs/{failure_job_id}

- 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**.
failure_job_id	Yes	Specifies the ID of a failed task. For details, see **Querying Failed Tasks**.

Request

- Request parameters

  None

- Example request

  DELETE https://{Endpoint}/v1/{project_id}/task-center/failure-jobs/897f57b2-6e94-4179-b414-9532726c59f2

Response

None

Returned Value

- Normal

Returned Value	Description
204	No Content

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.9.3 Deleting All Failed Tasks of All Protection Groups

Function

This API is used to delete all the failed tasks of the protection group level, such as failed protection group creation or deletion tasks.

URI

- URI format

  DELETE /v1/{project_id}/task-center/failure-jobs/batch

- Parameter description

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

Request

- Request parameters

  None

- Example request

  DELETE https://{Endpoint}/v1/{project_id}/task-center/failure-jobs/batch

Response

None

Returned Value

- Normal

Returned Value	Description
204	No Content

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.

Returned Value	Description
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.9.4 Deleting All Failed Tasks of a Protection Group

Function

This API is used to delete failed tasks in a protection group, such as failed protected instance creation or deletion tasks, and failed replication pair creation and deletion tasks.

Constraints and Limitations

- None

URI

- URI format

  DELETE /v1/{project_id}/task-center/{server_group_id}/failure-jobs/batch
- Parameter description

Parameter	Mandatory	Type	Description
project_id	Yes	String	Specifies the project ID. For details about how to obtain the project ID, see **Obtaining a Project ID**.
server_group_id	Yes	String	Specifies the ID of a protection group. For details, see **Querying Protection Groups**.

Request

- Request parameters

  None

- Example request

  DELETE https://{Endpoint}/v1/{project_id}/task-center/decf224d-87fe-403a-8721-037a1a45c287/failure-jobs/batch

Response

None

Returned Value

- Normal

Returned Value	Description
204	No Content

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not find the requested page.
405 Method Not Allowed	You are not allowed to use the method specified in the request.

Returned Value	Description
406 Not Acceptable	The response generated by the server could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

5.10 Tenant Quota Management

5.10.1 Querying the Tenant Quota

Function

This API is used to query the tenant quota.

Constraints and Limitations

None

URI

- URI format
  GET /v1/{project_id}/sdrs/quotas
- Parameter description

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

Request

- Request parameters

  None

- Example request

  GET https://{Endpoint}/v1/{project_id}/sdrs/quotas

Response

- Parameter description

Parameter	Type	Description
quotas	Object	Specifies the tenant quota information. For details, see **Table 5-73**.

Table 5-73 quotas field description

Parameter	Type	Description
resources	Array of objects	Lists the tenant's resource quota. For details, see **Table 5-74**.

Table 5-74 resources field description

Parameter	Type	Description
type	String	Specifies the resource type. The value can be **server_groups** or **replications**. ● **server_groups**: indicates protection groups. ● **replications**: indicates replication pairs.
used	Integer	Specifies the number of used resources.

Parameter	Type	Description
quota	Integer	Specifies the resource quota. If the value is **–1**, the resource is not limited.
min	Integer	Specifies the minimally allowed resource quota.
max	Integer	Specifies the maximally allowed resource quota. If the value is **–1**, the resource is not limited.

- Example response

```
{
    "quotas": {
        "resources": [
            {
                "type": "server_groups",
                "used": 10,
                "quota": 50,
                "min": 0,
                "max": -1
            },
            {
                "type": "replications",
                "used": 1,
                "quota": 100,
                "min": 0,
                "max": -1
            }
        ]
    }
}
```

Or

```
{
     "error": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

In this example, **error** represents a general error, including **badrequest** (shown below) and **itemNotFound**.

```
{
     "badrequest": {
         "message": "XXXX",
         "code": "XXX"
     }
 }
```

Returned Values

- Normal

Returned Value	Description
200	The server has accepted the request.

- Abnormal

Returned Value	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You must enter a username and the password to access the requested page.
403 Forbidden	You are forbidden to access the requested page.
404 Not Found	The server could not 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 could not be accepted by the client.
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 server receives an invalid response from an upstream server.
503 Service Unavailable	Failed to complete the request because the system is unavailable.
504 Gateway Timeout	A gateway timeout error occurred.

A Appendixes

A.1 Error Codes

If an error code starting with **APIGW** is returned after you call an API, rectify the fault by referring to the instructions provided in **Error Codes**.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.0001	Invalid tenant ID	The tenant ID is invalid.	Use a valid tenant ID.
400	SDRS.0002	Invalid tenant token	The tenant token is invalid.	Use a valid token.
400	SDRS.0003	Invalid roles	The tenant roles are invalid.	Check whether the tenant has the desired roles. If there are no desired roles, add them for the tenant. Check whether the roles have the required permissions using IAM.
400	SDRS.0004	Incorrect API invoking permissions	The user does not have the required permissions to invoke the interface.	Add the required permissions for the user. Check whether the roles of the user have the required permissions using IAM.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.0005	No permission for the operation	The user does not have the permission to perform the operation.	Add the required operation permission.
400	SDRS.0201	Invalid request parameters	The request parameters are invalid.	Use valid request parameters.
400	SDRS.0202	Invalid name	The name is invalid.	Use a valid name.
400	SDRS.0203	Invalid AZ	The AZ is invalid.	Use a valid AZ.
400	SDRS.0204	Invalid VPC	The VPC is invalid.	Use a valid VPC.
400	SDRS.0205	Invalid domain ID	The domain ID is invalid.	Use a valid domain ID.
400	SDRS.0206	Invalid action	The action is invalid.	Use a valid action.
400	SDRS.0207	Invalid protection group ID	The protection group ID is invalid.	Use a valid protection group ID.
400	SDRS.0208	Invalid protected instance ID	The protected instance ID is invalid.	Use a valid protected instance ID.
400	SDRS.0209	Incorrect status	The status is incorrect.	Ensure that the status is correct.
400	SDRS.0210	Invalid server ID	The server ID is invalid.	Use a valid server ID.
400	SDRS.0211	Invalid disk ID	The disk ID is invalid.	Use a valid disk ID.
400	SDRS.0212	Invalid description	The description is invalid.	Use a valid description.
400	SDRS.0213	Invalid replication pair ID	The replication pair ID is invalid.	Use a valid replication pair ID.
400	SDRS.0214	Incorrect replication pair status	The replication pair status is incorrect.	Ensure that the replication status is correct.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.0215	Invalid replication group ID	The replication consistency group ID is invalid.	Use a valid replication consistency group ID.
400	SDRS.0216	Invalid preferred AZ	The preferred AZ is invalid.	Use a valid AZ as the preferred AZ.
400	SDRS.0217	Invalid DR drill type	The DR drill type is invalid.	Use a valid DR drill type.
400	SDRS.0218	Invalid cluster ID	The cluster ID is invalid.	Use a valid cluster ID.
400	SDRS.0219	Invalid IP address	The IP address is invalid.	Use a valid IP address.
400	SDRS.0221	limit value must be greater than 0 or less than 1000	Invalid **limit** value. The value must be greater than 0 and less than 1000.	Use a valid **limit** value.
400	SDRS.0222	**offset** value cannot be negative, and must be an integer	Invalid **offset** value. The value cannot be negative and must be an integer.	Use a valid **offset** value.
400	SDRS.0223	Invalid NIC ID	Invalid NIC ID.	Use a valid NIC ID.
400	SDRS.0224	Invalid replication model.	The replication model is invalid.	Use a valid replication model.
400	SDRS.0225	Frozen volume	The volume has been frozen.	Use a volume that is not frozen.
400	SDRS.0226	IDs exceed the upper limit	The number of IDs exceeds the upper limit.	Set an ID list with at most 30 IDs.
400	SDRS.0227	Invalid **dedicated_host_id**.	**dedicated_host_id** is invalid.	Use valid **dedicated_host_id**.
400	SDRS.0228	Invalid **tenancy** value	The **tenancy** value is invalid.	**tenancy** can be set only to **shared** or **dedicated**.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.0231	No access permission for the source AZ	You do not have the permission to access the source AZ.	Contact customer service to add the permission.
400	SDRS.0232	No access permission for the target AZ	You do not have the permission to access the target AZ.	Contact customer service to add the permission.
400	SDRS.0233	No available active-active domain	No active-active domain is available.	Contact customer service to add the permission.
400	SDRS.0301	Invalid quota resource name	The quota resource name is invalid.	Use a valid quota resource name.
400	SDRS.0302	Invalid quota value	The quota value is invalid.	Use a valid quota value.
400	SDRS.0303	Quota value less than used resources	The quota value is less than the quantity of used resources.	Use a valid quota value.
400	SDRS.0304	Quota value greater than the maximum or less than the minimum	The quota value is greater than the maximum value or less than the minimum value.	Use a valid quota value.
500	SDRS.0006	Failed to obtain the token for the tenant	Failed to obtain the token for the tenant.	Check the user permission.
500	SDRS.0007	Failed to upgrade the permission	Failed to upgrade the permission.	Check whether the administrator account is used to upgrade the permission and whether the account is locked.
500	SDRS.0008	Network connection timeout	Network connection timed out.	Try again. If the retry fails, check the network status. If the network is normal, contact customer service.

Status Code	Error Code	Error Message	Description	Handling Measure
500	SDRS.0009	No permission for the operation	The user does not have the permission to perform the operation.	Check whether the user permission is limited.
500	SDRS.0010	Data error	Data error.	Contact customer service.
500	SDRS.0011	Client error	Client error.	Contact customer service.
500	SDRS.0012	Incorrect configuration	The configuration is incorrect.	Contact customer service.
500	SDRS.0013	Internal error	Internal error.	Contact customer service.
500	SDRS.0014	Null result of decoded tenant token	The result of decoding the tenant token is null.	Use a correct token.
500	SDRS.0015	Null or empty domain ID decoded from token	The domain ID decoded from the tenant token is null or empty.	Use a correct token.
500	SDRS.0016	Null or empty domain name decoded from token	The domain name decoded from the tenant token is null or empty.	Use a correct token.
500	SDRS.0401	Incorrect number of subjobs	The number of subjobs is incorrect.	Contact customer service.
500	SDRS.0402	Error occurred when submitting the subjob again	An error occurred when submitting the subjob again.	Contact customer service.
500	SDRS.0403	Error occurred during job context query	An error occurred when querying the job context.	Contact customer service.
500	SDRS.0404	Failed to submit the job	Failed to submit the job.	Contact customer service.

Status Code	Error Code	Error Message	Description	Handling Measure
500	SDRS.0405	Failed to execute the job	Failed to execute the job.	Contact customer service.
500	SDRS.0406	Failed to execute the subjob	Failed to execute the subjob.	Contact customer service.
500	SDRS.0407	Failed to roll back the job	Failed to roll back the job.	Contact customer service.
500	SDRS.0408	Null job	The job is null.	Contact customer service.
400	SDRS.1001	Protection group deletion not allowed due to a protected instance	The protection group cannot be deleted because it contains a protected instance.	Delete the protected instance from the protection group and then delete the protection group.
400	SDRS.1002	Operation not allowed for the protection group in the current state	This operation cannot be performed for the protection group in the current state.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1003	Protection group deletion not allowed due to a DR drill	The protection group cannot be deleted because it contains a DR drill.	Delete the DR drill from the protection group and then delete the protection group.
400	SDRS.1010	Protection group deletion not allowed due to a replication pair	The protection group cannot be deleted because it contains a replication pair.	Delete the replication pair from the protection group and then delete the protection group.
400	SDRS.1013	Protection group not found	The protection group is not found.	Use an available protection group.
400	SDRS.1015	Abnormal protection group data	The protection group data is abnormal.	Check the data of the protection group. If the fault persists, contact customer service.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1017	Operation not allowed because the protection group status not available	This operation cannot be performed because the protection group status is not available.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1018	Operation not allowed because the protection status of the protection group not stopped	This operation cannot be performed because the protection status of the protection group is not stopped.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1019	Operation not allowed because the protection status of the protection group not started	This operation cannot be performed because the protection status of the protection group is not started.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1020	Operation not allowed because the protection group status not available or starting	This operation cannot be performed because the protection group status is not available or starting.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1021	Operation not allowed because the protection group status not available, failed-over, or failed-over-back	This operation cannot be performed because the protection group status is not available, failed-over, or failed-over-back.	Perform this operation in the correct state and be clear about the operation restrictions.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1022	Operation not allowed because the protection group status not available, error-failing-over, or error-failing-over-back	This operation cannot be performed because the protection group status is not available, error-failing-over, or error-failing-over-back.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1023	Operation not allowed because the protection group status not available, error-reversing, or error-failing-back	This operation cannot be performed because the protection group status is not available, error-reversing, or error-failing-back.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1024	Operation not allowed because the protection group status not available or protected	This operation cannot be performed because the protection group status is not available or protected.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1025	**priority station** value of the protection group is different from that of the protected instance	The **priority station** value of the protection group is different from that of the protected instance.	Contact customer service.
400	SDRS.1026	**priority station** value of the protection group is different from that of the replication pair	The **priority station** value of the protection group is different from that of the replication pair.	Contact customer service.
400	SDRS.1027	Failed to enable protection	Failed to enable protection.	Try again. If the fault persists, contact customer service.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1028	Failed to disable protection	Failed to disable protection.	Try again. If the fault persists, contact customer service.
400	SDRS.1029	Failed to perform the planned failover	Failed to perform the planned failover for the protection group.	Try again. If the fault persists, contact customer service.
400	SDRS.1030	Failed to perform the failover	Failed to perform the failover for the protection group.	Try again. If the fault persists, contact customer service.
400	SDRS.1032	Failed to enable protection again	Failed to enable reprotection for the protection group.	Try again. If the fault persists, contact customer service.
400	SDRS.0305	Insufficient protection group quota	The protection group quota is insufficient.	Contact customer service to increase the quota.
500	SDRS.1011	Failed to query the active-active domain	Failed to query the active-active domain.	Try again. If the fault persists, contact customer service.
500	SDRS.1014	Failed to create the protection group	Failed to create the protection group.	Contact customer service.
500	SDRS.1016	Failed to delete the protection group	Failed to delete the protection group.	Contact customer service.
400	SDRS.1301	Protected instance deletion not allowed in the current state	The protected instance cannot be deleted in the current state.	Perform this operation in the correct state and be clear about the operation restrictions.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1303	Server AZ and production site AZ of the protection group are different	The server AZ and the production site AZ of the protection group are different.	Ensure that the server AZ is the same as the production site AZ of the protection group. For example, if the production site AZ of the protection group is AZ1, ensure that the production site server AZ is AZ1.
400	SDRS.1304	VPC of the server inconsistent with that of the protection group	The VPC of the server and the VPC of the protection group are different.	Ensure that the VPC of the server is the same as that of the protection group.
400	SDRS.1305	Server already used to create a protected instance	The server has been used to create a protected instance.	One server can be used to create only one protected instance. Select a server not used in any protected instance and create the instance again.
400	SDRS.1306	Failed to create the server	Failed to create the server.	Try again. If the fault persists, contact customer service.
400	SDRS.1307	Failed to delete the server	Failed to delete the server.	Try again. If the fault persists, contact customer service.
400	SDRS.1308	Failed to stop the server	Failed to stop the server.	Try again. If the fault persists, contact customer service.
400	SDRS.1309	Inconsistent production site and DR site disk specifications	Specifications of the production site disk and DR site disk are different.	Check whether the specifications of the production site and DR site disks of the protected instance are consistent. If they are not, contact customer service.
400	SDRS.1310	NIC not exist	The NIC does not exist.	Use an available NIC.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1311	Deleting the primary NIC not allowed	The primary NIC cannot be deleted.	Check whether the NIC is the primary one. If it is, it cannot be deleted.
400	SDRS.1312	Failed to add the NIC to the protected instance	Failed to add the NIC to the protected instance.	Try again. If the fault persists, contact customer service.
400	SDRS.1313	Failed to delete the NIC from the protected instance	Failed to delete the NIC from the protected instance.	Try again. If the fault persists, contact customer service.
400	SDRS.1314	Abnormal protected instance	The protected instance is abnormal.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1315	Extension NIC not found	The extension NIC is not found.	Check whether the extension NIC is normal. Use the correct extension NIC, or contact customer service.
400	SDRS.1316	Server not stopped	The server is not stopped.	Check whether the server is stopped. If it is working, stop it.
400	SDRS.1317	Failed to attach the NIC to a protected instance	Failed to attach the NIC to the protected instance.	Try again. If the fault persists, contact customer service.
400	SDRS.1318	Failed to detach the NIC from a protected instance	Failed to detach the NIC from the protected instance.	Try again. If the fault persists, contact customer service.
400	SDRS.1319	Server at the current production site not stopped	The current production site server is not stopped.	Check whether the current production site server is stopped. If not, stop it.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1320	Protected instance not found	The protected instance is not found.	Use an available protected instance.
400	SDRS.1321	No disk attached to the server	No disk is attached to the server.	Check whether disks are attached to the server and be clear about the operation constraints.
400	SDRS.1322	Abnormal system disk of the server	The system disk of the server is abnormal.	Contact customer service.
400	SDRS.1323	Protected instance creation not allowed because the protection group status not available	Protected instances cannot be created because the protection group status is not available.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1324	Protected instance deletion not allowed because the protection group status not available	Protected instances cannot be deleted because the protection group status is not available.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1325	Protected instance creation not allowed because the protection group status not stopped	Protected instances cannot be created because the protection group status is not stopped.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1326	Server not found	The server is not found.	Use an available server.
400	SDRS.1327	NIC-related operation not allowed for the protected instance state in the current state	The NIC-related operation cannot be performed for the protected instance in the current state.	Perform this operation in the correct state and be clear about the operation restrictions.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1328	Operation not allowed because the protected instance status not available	This operation cannot be performed because the protected instance status is not available.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1329	Failed to modify protected instance specifications	Failed to modify the specifications of the protected instance.	Try again. If the fault persists, contact customer service.
400	SDRS.1330	Server at the current production site cannot be deleted because the current production site not the one specified when the protection group is created	The server at the current production site cannot be deleted because the current production site is not the one specified when the protection group is created.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1331	Failed to delete the EIP	Failed to release the EIP.	Try again. If the fault persists, contact customer service.
400	SDRS.1332	Failed to add the EIP	Failed to add the EIP.	Try again. If the fault persists, contact customer service.
400	SDRS.1333	Operation not allowed because the server status is not active or shutoff	A protected instance cannot be created when the server status is not active or shutoff.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1334	Private IP address in the subnet is in use	The private IP address is already in use.	Check whether the private IP address is in use.
400	SDRS.1335	Subnet not found	The subnet was not found.	Use a correct subnet.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1336	Protected instance cannot be created using a production site server attached with an extension NIC in the current system	In the current system, a protected instance cannot be created using a production site server attached with an extension NIC.	Delete the extension NIC or select the correct production site server.
400	SDRS.1337	Current system does not support the extension NIC to be added to the protected instance	In the current system, extension NICs cannot be added to protected instances.	Be clear about the operation constraints.
400	SDRS.1338	Failed to delete the EIP of the current production site server because the current production site is not the one specified when the protection group is created	The EIP of the current production site server cannot be deleted because the current production site is not the one specified when the protection group is created.	Be clear about the operation constraints.
400	SDRS.1339	No system disk attached to the server	No system disk is attached to the server.	Check whether a system disk is attached to the server and be clear about the operation constraints.
400	SDRS.1340	Number of NICs for one protected instance reaches the upper limit	The number of NICs for one protected instance reaches the upper limit.	Check whether the number of NICs for one protected instance reaches the upper limit and be clear about the operation constraints.
400	SDRS.1341	Another flavor must be used for resizing	This flavor cannot be used for the flavor change.	The target flavor is the same as the current one. Select another flavor for the flavor change.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1342	Current DR site server is not stopped	The current DR site server is not stopped.	Check whether the current DR site server is stopped. If not, contact the administrator to stop it.
400	SDRS.1350	Failed to create the protected instance	Failed to create the protected instance.	Try again. If the fault persists, contact customer service.
400	SDRS.1351	Failed to delete the protected instance	Failed to delete the protected instance.	Try again. If the fault persists, contact customer service.
400	SDRS.1352	Current production site server not stopped	The current production site server is not stopped.	Check whether the current production site server is stopped. If not, stop it and then perform the operation.
400	SDRS.1353	DR site server specifications not support protected instance creation	The DR site server specifications do not support the creation of a protected instance.	Use a server of other specifications to create a protected instance.
400	SDRS.1354	DR site server in protected instance cannot be deleted because the billing mode for the DR site server is yearly/monthly	The billing mode of the DR site server in the protected instance is yearly/monthly. Therefore, the DR site server cannot be deleted when you delete the protected instance.	If the billing mode of the DR site server in the protected instance is yearly/monthly, do not select **Delete DR site server** when you delete the protected instance. If the fault persists, contact customer service.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1355	Failed to delete the DR site server in the protected instance because the current account is frozen	Failed to delete the DR site server in the protected instance because the current account is frozen.	Do not select **Delete DR site server**, or wait until your account is unfrozen and then perform the operation.
400	SDRS.1356	Production site server specifications not support protected instance creation	The production site server specifications do not support the creation of a protected instance.	Use a server of other specifications to create a protected instance.
400	SDRS.1357	Production site server locked by system	The production site server is locked by the system.	Check whether the current production site server is locked by the system. If so, wait until the server is unlocked and then perform the operation.
400	SDRS.1358	Number of protected instances in the protection group reaches the upper limit	The number of protected instances in the protection group reaches the upper limit.	Select another protection group to create a protected instance.
400	SDRS.1359	Production site server locked by another cloud service	The production site server is locked by another cloud service.	Check whether the current production site server is locked by another cloud service. If so, wait until the server is unlocked and then perform the operation.
400	SDRS.1360	**servers** configuration contains an invalid production site server ID	The **servers** configuration contains an invalid server ID.	Specify correct production site server IDs.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1361	**servers** configuration contains a duplicate production site server ID	The **servers** configuration contains a duplicate server ID.	Delete the duplicate server ID.
400	SDRS.1362	Number of production site servers in the **servers** configuration exceeds the upper limit	The number of production site servers in the **servers** configuration exceeds the upper limit.	Reduce the number of production site servers and try again.
400	SDRS.1363	**protected_instances** configuration contains a duplicate protected instance ID	The **protected_instances** configuration contains a duplicate protected instance ID.	Delete the duplicate protected instance ID.
400	SDRS.1364	**protected_instances** configuration contains IDs of protected instances from different protection groups	The **protected_instances** configuration contains IDs of protected instances from different protection groups.	Ensure that the IDs of protected instances are from the same protection group and then try again.
400	SDRS.1365	Failed to delete the protected instance because a shared replication pair attached to this protected instance is attached to another protected instance	Failed to delete the protected instance because a shared replication pair attached to this protected instance has been attached to other protected instances.	Detach the shared replication pair from the protected instance and then try again.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1366	System not support creating DR site servers on DeHs	In the current system, DeHs cannot be used to create DR site servers.	Delete the DeH parameters and try again.
400	SDRS.1367	Failed to specify the DeH parameters when you modify specifications of DR site servers not created on DeHs	DeH parameters are not supported if the DR site servers you want to modify specifications are not created on DeHs.	Delete the DeH parameters and try again.
400	SDRS.1368	Failed to specify the DeH parameters when you modify specifications of production site servers not created on DeHs	DeH parameters are not supported if the production site servers you want to modify specifications are not created on DeHs.	Delete the DeH parameters and try again.
400	SDRS.1369	DeH ID of the DR site server is empty	The DeH ID of the DR site server is empty.	Use a correct DeH ID.
400	SDRS.1370	DeH ID of the production site server is empty	The DeH ID of the production site server is empty.	Use a correct DeH ID.
400	SDRS.1371	**dedicated_host_id** cannot be specified when **tenancy** is set to **shared**	**dedicated_host_id** cannot be specified when **tenancy** is set to **shared**.	Delete **dedicated_host_id** and try again.
400	SDRS.1372	DeH not found	The DeH is not found.	Use a correct DeH ID.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1373	DeH AZ and the DR site AZ of the protection group are different	The DeH AZ and the DR site AZ of the protection group are different.	Verify that the DeH AZ is the same as the DR site AZ of the protection group. For example, if the DR site AZ of the protection group is AZ1, ensure that the DeH AZ is AZ1.
400	SDRS.1374	Failed to create a DR site server of such specifications on a DeH	Failed to create a DR site server of such specifications on a DeH.	Use the supported specifications setting.
400	SDRS.1375	Failed to create a DR site server on the DeH because the production site server belongs to an ECS group	Failed to create a DR site server on the DeH because the production site server belongs to an ECS group.	Remove the production site server from the ECS group and try again.
400	SDRS.1376	Failed to modify the specifications because the servers of the protected instance are billed in yearly/monthly mode	Failed to modify the specifications because the servers of the protected instance are billed in yearly/monthly mode.	Delete the protected instance and then change the server specifications.
400	SDRS.1377	Failed to modify the specifications because the protected instance does not have a replication pair containing system disks attached	Failed to modify the specifications because the protected instance is not attached with a replication pair consisting of system disks.	Attach a replication pair consisting of system disks to the protected instance and then try again.
400	SDRS.1378	Failed to modify the specifications of the production site server to the current ones	Failed to modify the specifications of the production site server to the current one.	Use the supported specifications setting.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1379	Failed to modify the specifications of the DR site server to the current ones	Failed to modify the specifications of the DR site server to the current one.	Use the supported specifications setting.
400	SDRS.1380	**primary_subnet_id** must be specified when **primary_ip_address** is specified	**primary_subnet_id** must be specified if **primary_ip_address** is specified.	Specify **primary_subnet_id** and try again.
400	SDRS.1381	DSS storage pool ID not exist	The DSS storage pool ID does not exist.	Use an available DSS storage pool ID.
400	SDRS.1382	DR site not support DSS	The DR site does not support DSS.	Delete the DSS storage pool ID and try again.
400	SDRS.1383	DSS storage pool AZ and the DR site AZ of the protection group are different	The DSS storage pool AZ and the DR site AZ of the protection group are different.	Verify that the DSS storage pool AZ is the same as the DR site AZ of the protection group. For example, if the DR site AZ of the protection group is AZ1, ensure that the DSS storage pool AZ is AZ1.
400	SDRS.1384	DSS storage pool is being deployed and cannot be used	DSS storage pool is being deployed and cannot be used.	Wait until the DSS storage pool deployment succeeded and try again.
400	SDRS.1385	Insufficient capacity of the DSS storage pool	The DSS storage pool capacity is not enough.	Expand the DSS storage pool or select another pool with enough capacity.
400	SDRS.1386	Storage type of the DSS storage pool is different from the disk type of the production site	The DSS storage pool type is different from the disk type of the production site.	Select a DSS storage pool with the storage type same as the disk type of the production site.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1408	A server with the shared disk attached is not in the server list for which the protected instances are to be protected	A server with the shared disk attached is not in the server list available for creating protected instances.	Check the attachment information of the shared disk and ensure that all the servers with the shared disk attached are in the list.
400	SDRS.1409	A protected instance with the shared replication pair attached is not in the deletion list	A protected instance with the shared replication pair attached is not in the protected instance list available for deletion.	Check the attachment information of the replication pair and ensure that all the protected instances with the shared replication pair attached are in the list.
400	SDRS.1601	Replication pair status not available	The replication pair status is not available.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1603	Replication pair attached or device name used to attach to a disk	The replication pair has been attached, or the device name has been used.	Use an available replication pair or device name.
400	SDRS.1604	Replication pair not attached	The replication pair is not attached.	Check the replication pair attachment status and be clear about the operation constraints.
400	SDRS.1605	Replication pair attached	The replication pair has been attached.	Check the replication pair attachment status and be clear about the operation constraints.
400	SDRS.1606	Failed to create the replication pair and status being error	The replication pair failed to be created and its status is error.	Contact customer service.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1607	Failed to delete the replication pair	The replication pair failed to be deleted and its status is error-deleting.	Contact customer service.
400	SDRS.1608	Replication pair not found	The replication pair is not found.	Use an available replication pair.
400	SDRS.1609	Replication pair creation failure	Failed to create the replication pair.	Try again. If the fault persists, contact customer service.
400	SDRS.1610	Replication pair update failure	Failed to update the replication pair.	Try again. If the fault persists, contact customer service.
400	SDRS.1611	Replication pair not in the protection group	The replication pair is not in the protection group.	Use an available protection group.
400	SDRS.1801	Disk status not available	The disk status is not available.	Perform this operation in the correct state and be clear about the operation restrictions.
400	SDRS.1802	Disk encrypted	The disk is an encrypted disk.	Check whether the disk is an encrypted disk. An encrypted disk cannot be used to create a replication pair.
400	SDRS.1803	Null disk	The disk is null.	Use a correct disk.
400	SDRS.1804	Disk not attached	The disk is not attached.	Check whether the disk is attached.
400	SDRS.1805	Disk not used for creating replication pair	The disk is not used for creating a replication pair.	Check whether the disk is used for creating a replication pair.
400	SDRS.1806	Operation not allowed by disk type	The disk type does not allow this operation.	Check the disk type and ensure that you use a correct disk type.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1807	Disks failed to be attached to the server	Disks failed to be attached to the server.	Try again. If the fault persists, contact customer service.
400	SDRS.1808	Disks failed to be detached from the server	Disks failed to be detached from the server.	Try again. If the fault persists, contact customer service.
400	SDRS.1809	Operation not allowed because the current production site of the replication pair is the DR site specified when the protection group is created	This operation cannot be performed because the current production site of the replication pair is the DR site specified when the protection group was created.	Perform a planned failback or failback, and then try again.
400	SDRS.1810	Current production site AZ of the disk different from that of the protection group	The current production site AZ of the disk is different from that of the protection group.	Select a disk with its production site AZ same as that of the protection group, and then try again.
400	SDRS.1811	Disk already used by a replication pair	The disk has been used by a replication pair.	Select a disk not used by a replication pair, and then try again.
400	SDRS.1812	Failed to create the disk	Failed to create the disk.	Try again. If the fault persists, contact customer service.
400	SDRS.1813	Failed to delete the disk	Failed to delete the disk.	Try again. If the fault persists, contact customer service.
400	SDRS.1814	Disk size is different	Disk sizes are different.	Try again. If the fault persists, contact customer service.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1816	Operation cannot be performed because the disk of the replication pair is not in the available state	The replication pair capacity cannot be expanded because the disks on the replication pair are not in the available state.	If the replication pair has been attached to a protected instance, detach the replication pair first. If the problem persists, contact customer service.
400	SDRS.1817	Operation cannot be performed because the disk of the replication pair is not in the available or in-use state	The replication pair capacity cannot be expanded because the disks of the replication pair are not in the available or in-use state.	Try again. If the fault persists, contact customer service.
400	SDRS.1818	This operation cannot be performed because the shared disks of the replication pair are not in the Available state	The replication pair capacity cannot be expanded because the shared disks of the replication pair are not in the available state.	If the replication pair has been attached to a protected instance, detach the replication pair first. If the problem persists, contact customer service.
400	SDRS.0306	Insufficient replication pair quota	The replication pair quota is insufficient.	Contact customer service to increase the replication pair quota.
400	SDRS.1819	Replication pair capacity cannot be expanded because the billing mode for the disks of the replication pair is yearly/monthly	The replication pair capacity cannot be expanded because the billing mode for the disks of the replication pair is yearly/monthly.	Delete the replication pair, expand the production site disk, and then use the disk to create a new replication pair.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1820	Failed to expand the capacity	Failed to expand the capacity of the replication pair.	Try again. If the fault persists, contact customer service.
400	SDRS.1821	Failed to attach the replication pair	Failed to attach the replication pair.	Try again. If the fault persists, contact customer service.
400	SDRS.1822	Failed to detach the replication pair	Failed to detach the replication pair.	Try again. If the fault persists, contact customer service.
400	SDRS.1823	Operation not allowed due to a system error	This operation cannot be performed due to a system error.	Perform a failover or contact customer service.
400	SDRS.1824	Operation not allowed due to a system error	This operation cannot be performed due to a system error.	Contact customer service.
400	SDRS.1825	Disk already used in a DR drill	The disk is already used in a DR drill.	Use an available disk.
400	SDRS.1826	Replication pairs not attached to protected instances to the upper limit	The number of replication pairs that are not attached to any protected instances reaches the upper limit.	Delete replication pairs that are not attached to any protected instance, or attach them and then create new replication pairs. If the fault persists, contact customer service.
400	SDRS.1827	DR site disk in replication pair cannot be deleted because the billing mode for the disk is yearly/monthly	The billing mode of the DR site disk in the replication pair is yearly/monthly. Therefore, the DR site disk cannot be deleted when you delete the replication pair.	Do not select **Delete DR site disk** when deleting the replication pair. If the fault persists, contact customer service.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1828	Failed to delete the DR site disk in the replication pair because the current account is frozen	Failed to delete the DR site disk in the replication pair because the current account is frozen.	Do not select **Delete DR site disk**, or wait until your account is unfrozen and then perform the operation.
400	SDRS.1830	Operation not allowed because replication pairs in this protection group are synchronizing data	This operation cannot be performed because replication pairs in this protection group are synchronizing data.	Wait until the synchronization of all replication pairs in the protection group is complete and then perform the operation.
400	SDRS.1831	Disk locked	The disk is locked.	Check whether the disk is locked. If so, wait until the disk is unlocked and then perform the operation.
400	SDRS.1832	Failed to expand the capacity because a disk in the replication pair is locked	Failed to expand the capacity because a disk in the replication pair is locked.	Check whether the disk is locked. If so, wait until the disk is unlocked and then perform the operation.
400	SDRS.1900	Invalid DR drill ID	The DR drill ID is invalid.	Use a valid DR drill ID.
400	SDRS.1901	Null or empty DR drill ID	The DR drill ID is null or empty.	Use a valid DR drill ID.
400	SDRS.1902	DR drill not found	The DR drill is not found.	Use an available DR drill.
500	SDRS.1904	Snapshot not found	The snapshot is not found.	Use an available snapshot.
500	SDRS.1905	Failed to create a volume using the snapshot	Failed to create a disk using the snapshot.	Contact customer service.
500	SDRS.1906	Failed to delete the snapshot	Failed to delete the snapshot.	Contact customer service.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1907	Drill VPC conflicts with the VPC of the protection group	The drill VPC conflicts with the VPC of the protection group.	Use a correct drill VPC.
400	SDRS.1908	Drill VPC not have a subnet	The drill VPC does not have a subnet.	Use a correct VPC or create a subnet same as that in the VPC of the protection group. If the fault persists, contact customer service.
400	SDRS.1909	Drill VPC not have the CIDR block	The drill VPC does not have the CIDR block.	Ensure that the drill VPC has the same CIDR block with the VPC of the protection group. If the fault persists, contact customer service.
400	SDRS.1910	IP addresses in the drill VPC conflict	The IP addresses in the drill VPC conflict.	Contact customer service.
400	SDRS.1911	Null or empty NIC	The NIC is null or empty.	Contact customer service.
500	SDRS.1912	Failed to create the drill NIC	Failed to create the drill NIC.	Contact customer service.
400	SDRS.1913	DR drill deletion not allowed in the current state	The DR drill cannot be deleted in the current state.	Perform this operation in the correct state and be clear about the operation restrictions.
500	SDRS.1914	Drill server record not found	The drill server record is not found.	Contact customer service.
500	SDRS.1915	Drill storage record not found	The drill storage record is not found.	Contact customer service.
500	SDRS.1916	Invalid snapshot ID	The snapshot ID is invalid.	Contact customer service.

Status Code	Error Code	Error Message	Description	Handling Measure
500	SDRS.1917	Drill NIC record not found	The drill NIC record is not found.	Contact customer service.
500	SDRS.1918	Failed to delete the drill NIC	Failed to delete the drill NIC.	Contact customer service.
500	SDRS.1919	Failed to query the attachment information of the drill server	Failed to query the attachment information of the drill server.	Contact customer service.
500	SDRS.1920	Null attachment information of the replication pair for creating the DR drill	The attachment information of the replication pair for creating the DR drill is null.	Contact customer service.
400	SDRS.1921	Drill VPC is already used for creating a DR drill	The drill VPC is already used for creating a DR drill.	Use another available drill VPC.
400	SDRS.1922	Failed to create the DR drill	Failed to create the DR drill.	Try again. If the fault persists, contact customer service.
400	SDRS.1923	Failed to delete the DR drill	Failed to delete the DR drill.	Try again. If the fault persists, contact customer service.
400	SDRS.1924	DR site VPC not have a subnet	The DR site VPC does not have a subnet.	Contact customer service.
400	SDRS.1925	Failed to create the drill VPC	Failed to create the drill VPC.	Try again. If the fault persists, contact customer service.
400	SDRS.1926	Failed to create the subnet in the drill VPC	Failed to create the subnet in the drill VPC.	Try again. If the fault persists, contact customer service.
400	SDRS.1927	Failed to delete the subnet in the drill VPC	Failed to delete the subnet in the drill VPC.	Try again. If the fault persists, contact customer service.
400	SDRS.1928	Failed to find the VPC	Failed to find the VPC.	Contact customer service.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.1929	Insufficient VPC quota	The VPC quota is insufficient.	Delete unused VPCs or contact customer service to increase the VPC quota.
400	SDRS.1930	Insufficient subnet quota	The subnet quota is insufficient.	Delete unused subnets or customer service to increase the subnet quota.
400	SDRS.2201	**action** only **create** or **delete**	**action** can be set to **create** or **delete** only.	Enter the correct parameter value and then try again.
400	SDRS.2202	Empty tag list	The tag list is empty.	Enter the correct parameter value and then try again.
400	SDRS.2203	Number of tags exceeds the upper limit	The number of tags exceeds the upper limit.	Enter the correct parameter value and then try again.
400	SDRS.2204	Invalid tag key	The tag key is invalid.	Enter the correct parameter value and then try again.
400	SDRS.2205	Tag key is blank or an empty string	The tag key is left blank or an empty string.	Enter the correct parameter value and then try again.
404	SDRS.2206	Specified tag key is not found	The specified tag key is not found.	Enter the correct parameter value and then try again.
400	SDRS.2207	Invalid tag value	The tag value is invalid.	Enter the correct parameter value and then try again.
400	SDRS.2208	Null tag value	The tag value is null.	Enter the correct parameter value and then try again.
400	SDRS.2209	Tag parameter contains duplicate keys	Tags contain duplicate keys.	Enter the correct parameter value and then try again.
400	SDRS.2210	**action** can be set to only **filter** or **count**	**action** can be set to **filter** or **count** only.	Enter the correct parameter value and then try again.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.2211	**limit** and **offset** are not supported when **action** is set to **count**	**limit** and **offset** are not supported if **action** is set to **count**.	Enter the correct parameter value and then try again.
400	SDRS.2212	Empty **matches** parameter	The **matches** parameter is left blank.	Enter the correct parameter value and then try again.
400	SDRS.2213	Empty key in the **matches** parameter	The key in the **matches** parameter is left blank.	Enter the correct parameter value and then try again.
400	SDRS.2214	Invalid key in the **matches** parameter	The key in the **matches** parameter is invalid.	Enter the correct parameter value and then try again.
400	SDRS.2215	Duplicate keys in the **matches** parameter	The **matches** parameter contains duplicate keys.	Enter the correct parameter value and then try again.
400	SDRS.2216	Null value in the **matches** parameter	The value in the **matches** parameter is null.	Enter the correct parameter value and then try again.
400	SDRS.2217	Invalid value in the **matches** parameter	The value in the **matches** parameter is invalid.	Enter the correct parameter value and then try again.
400	SDRS.2218	Number of values exceeds the upper limit	The number of values exceeds the upper limit.	Enter the correct parameter value and then try again.
400	SDRS.2219	Value list of the same key has duplicate values	Duplicate values exist for the same key.	Enter the correct parameter value and then try again.
400	SDRS.2220	Minimum and maximum values of **limit** are **1** and **1000** respectively	Minimum and maximum values of **limit** are **1** and **1000** respectively.	Enter the correct parameter value and then try again.

Status Code	Error Code	Error Message	Description	Handling Measure
400	SDRS.2221	Tag adding not allowed in the current protected instance state	Tags cannot be added to the protected instance in the current state.	Ensure that the protected instance is normal and then try again.
400	SDRS.2222	Tag deleting not allowed in the current protected instance state	Tag cannot be deleted for the protected instance in the current state.	Ensure that the protected instance is normal and then try again.

A.2 Protection Group Status

Protection Group Status	Description
creating	The protection group is being created.
available	The protection group is available, and protection is disabled.
protected	Protection is enabled for the protection group.
deleting	The protection group is being deleted.
error-deleting	Failed to delete the protection group.
error	Failed to create the protection group.
starting	The protection group is being protected.
error-starting	Failed to enable protection for the protection group.
reprotecting	The protection group is being re-protected. When users enable protection after a failover or failback, the protection group status changes to re-protecting.
error-reprotecting	Failed to enable protection again for the protection group.
stopping	The system is stopping protection for the protection group.

Protection Group Status	Description
error-stopping	Failed to disable protection for the protection group.
reversing	The system is performing a planned failover on the protection group.
error-reversing	Failed to perform the planned failover.
failing-over	The system is performing a failover on the protection group.
failed-over	The failover is complete.
error-failing-over	Failed to perform the failover.

A.3 Protected Instance Status

Protected Instance Status	Description
creating	The protected instance is being created.
available	The protected instance is available.
deleting	The protected instance is being deleted.
error-deleting	Failed to delete the protected instance.
error	Failed to create the protected instance.
nic-creating	The system is adding a NIC to the protected instance.
nic-deleting	The system is deleting a NIC from the protected instance.
starting	Protection is being enabled for the protected instance.
error-starting	Failed to enable protection for the protected instance.
protected	Protection is enabled for the protected instance.
reversing	The system is performing a planned failover for the protected instance.
failing-over	The system is performing a failover for the protected instance.

Protected Instance Status	Description
failed-over	A failover is performed for the protected instance.
reprotecting	Protection is being enabled again for the protected instance. When users enable protection after a failover, the status changes to re-protecting.
stopping	Protection is being disabled for the protected instance.
error-stopping	Failed to disable protection for the protected instance.
error-reversing	Failed to perform the planned failover for the protected instance.
error-failing-over	Failed to perform the failover for the protected instance.
error-reprotecting	Failed to enable protection again for the protected instance.
resizing	The specifications of the protected instance are being modified.
error-resizing	Failed to modify the specifications of the protected instance.
invalid	A server in the protected instance has been deleted.
fault	The synchronization status of the replication pair for the protected instance is abnormal.

A.4 Replication Pair Status

Replication Pair Status	Description
creating	The replication pair is being created.
available	The replication pair is available.
deleting	The replication pair is being deleted.
error-deleting	Failed to delete the replication pair.
error	Failed to create the replication pair.

Replication Pair Status	Description
extending	The system is expanding the capacity of the replication pair.
error-extending	Failed to expand the capacity of the replication pair.
starting	The system is enabling protection for the replication pair.
error-starting	Failed to enable protection for the replication pair.
protected	Protection is enabled for the replication pair.
reversing	The system is performing a planned failover for the replication pair.
failing-over	The system is performing a failover for the replication pair.
failed-over	Failover is performed for the replication pair.
reprotecting	The system is enabling protection again for the replication pair. When users enable protection after a failover, the status changes to re-protecting.
stopping	The system is disabling protection for the replication pair.
error-stopping	Failed to disable protection for the replication pair.
error-reversing	Failed to perform a planned failover for the replication pair.
error-failing-over	Failed to perform a failover for the replication pair.
error-reprotecting	Failed to enable protection again for the replication pair.
invalid	A disk in the replication pair has been deleted.
fault	The synchronization status of the replication pair is abnormal.
attaching	The system is attaching the replication pair to a protected instance.

Replication Pair Status	Description
detaching	The system is detaching the replication pair from a protected instance.
error-attaching	Failed to attach the replication pair to a protected instance.
error-detaching	Failed to detach the replication pair from a protected instance.

A.5 DR Drill Status

DR Drill Status	Description
creating	The DR drill is being created.
available	The DR drill is available.
deleting	The DR drill is being deleted.
error-deleting	Failed to delete the DR drill.
error	Failed to create the DR drill.

A.6 Obtaining a Project ID

Scenarios

A project ID is required for some URLs when an API is called. Therefore, you need to obtain a project ID in advance. Two methods are available:

- **Obtain the Project ID by Calling an API**
- **Obtain the Project ID from the Console**

Obtain the Project ID by Calling an API

You can obtain a project ID by calling the API used to **query projects based on specified criteria**.

The API used to obtain a project ID is GET https://{Endpoint}/v3/projects. {Endpoint} is the IAM endpoint and can be obtained from **Regions and Endpoints**. For details about API authentication, see **Authentication**.

The following is an example response. The value of **id** is the project ID.

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

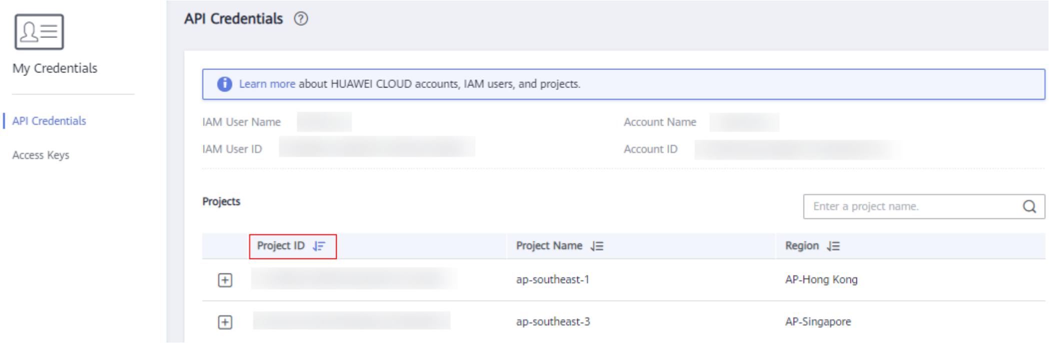
Obtain a Project ID from the Console

To obtain a project ID from the console, perform the following operations:

1. Log in to the management console.
2. Click the username and select **My Credentials** from the drop-down list.

   On the **API Credentials** page, view the project ID in the project list.

Figure A-1 Viewing the project ID



Learn more about HUAWEI CLOUD accounts, IAM users, and projects.

IAM User Name [redacted] Account Name [redacted]

IAM User ID [redacted] Account ID [redacted]

Projects

Enter a project name.

	Project ID	Project Name	Region
⊞	[redacted]	ap-southeast-1	AP-Hong Kong
⊞	[redacted]	ap-southeast-3	AP-Singapore

B Change History

Released On	Description
2020-04-29	This issue is the fifth official release. Modified the following content: ● Modified restrictions in **Creating a Protected Instance** and **Batch Deleting Protected Instances**. Specifically, shared disks are supported. ● Added error codes SDRS.0231, SDRS.0232, SDRS.0233, SDRS.1408, and SDRS.1409 in **Error Code Description**.
2019-11-30	This issue is the fourth official release. Modified the following content: Unified the parameter types in the parameter description tables.
2019-10-30	This issue is the third official release. Added the following content: ● **Batch Creating Protected Instances** ● **Batch Deleting Protected Instances** Modified the following content: ● Added descriptions about DeHs and parameters **tenancy** and **dedicated_host_id** in **Creating a Protected Instance**. ● Added parameters **production_dedicated_host_id** and **dr_dedicated_host_id** and request examples in **Modifying the Specifications of a Protected Instance**. ● Added three common error codes SDRS.0218, SDRS.0227, and SDRS.0228, and 27 error codes about protected instances (SDRS.1360 to SDRS.1386) in **Error Codes**.

Released On	Description
2019-05-30	This issue is the second official release. Added the following content: - **Tag Management** Modified the following content: - Added field **sold_out** in **Querying an Active-Active Domain**. - Added error code including SDRS.1829, SDRS.1355, and SDRS.1356 in **Error Codes**.
2019-04-10	This issue is the first official release.