



Cloud Backup and Recovery

API Reference

Date 2021-09-30

Contents

1 Before You Start.....	1
1.1 Overview.....	1
1.2 API Calling.....	1
1.3 Endpoints.....	1
1.4 Constraints.....	2
1.5 Concepts.....	2
2 API Overview.....	4
3 Calling APIs.....	5
3.1 Making an API Request.....	5
3.2 Authentication.....	9
3.3 Response.....	10
4 CBR APIs.....	12
4.1 Tasks.....	12
4.1.1 Querying a Single Task.....	12
4.1.2 Querying the Task List.....	19
4.2 Backup Sharing.....	32
4.2.1 Adding a Share Member.....	32
4.2.2 Updating the Share Member Status.....	34
4.2.3 Querying Share Member Details.....	37
4.2.4 Obtaining the Share Member List.....	39
4.2.5 Deleting a Specified Share Member.....	42
4.3 Restore Points.....	43
4.3.1 Querying a Restore Point.....	43
4.3.2 Creating a Restore Point.....	47
4.4 Vaults.....	53
4.4.1 Creating a Vault.....	53
4.4.2 Querying a Specified Vault.....	66
4.4.3 Querying the Vault List.....	76
4.4.4 Modifying a Vault.....	83
4.4.5 Deleting a Vault.....	91
4.4.6 Dissociating Resources.....	92
4.4.7 Associating Resources.....	94

4.4.8 Applying a Policy to a Vault.....	96
4.4.9 Removing a Policy from a Vault.....	98
4.4.10 Migrating Resources.....	100
4.5 Backups.....	102
4.5.1 Querying a Specified Backup.....	102
4.5.2 Querying All Backups.....	107
4.5.3 Deleting a Backup.....	114
4.5.4 Restoring a Backup.....	116
4.6 Policies.....	118
4.6.1 Creating a Policy.....	118
4.6.2 Querying a Single Policy.....	128
4.6.3 Querying the Policy List.....	134
4.6.4 Modifying a Policy.....	140
4.6.5 Deleting a Policy.....	150
5 Application Cases.....	153
5.1 Example 1: Creating an ECS Backup.....	153
5.2 Example 2: Implementing Automatic Backup for a Vault.....	156
5.3 Example 3: Querying Backups.....	158
6 Permissions Policies and Supported Actions.....	161
6.1 Introduction.....	161
6.2 Category of CBR Actions.....	162
7 Appendix.....	167
7.1 Status Codes.....	167
7.2 Error Codes.....	168
7.3 Obtaining a Project ID.....	186
A Change History.....	188

1 Before You Start

- [1.1 Overview](#)
- [1.2 API Calling](#)
- [1.3 Endpoints](#)
- [1.4 Constraints](#)
- [1.5 Concepts](#)

1.1 Overview

Welcome to *Cloud Backup and Recovery API Reference*. Cloud Backup and Recovery (CBR) allows you to easily back up Elastic Cloud Servers (ECSs) and Elastic Volume Service (EVS) disks. If there is a virus attack, accidental deletion, or software or hardware fault, data can be restored to any point in the past when the data was backed up. With CBR, you can back up and restore data on the cloud.

You can use APIs provided in this document to perform operations on CBR, such as creating and deleting a vault, and creating a policy. For details about all supported operations, see [2 API Overview](#).

Before calling CBR APIs, ensure that you have fully understood relevant concepts. For details, see section "Service Overview" in the *Cloud Backup and Recovery User Guide*.

1.2 API Calling

CBR supports Representational State Transfer (REST) APIs, allowing you to call APIs using HTTPS. For details about API calling, see [Making an API Request](#).

1.3 Endpoints

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

1.4 Constraints

For more constraints, see API description.

1.5 Concepts

- **Account**

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

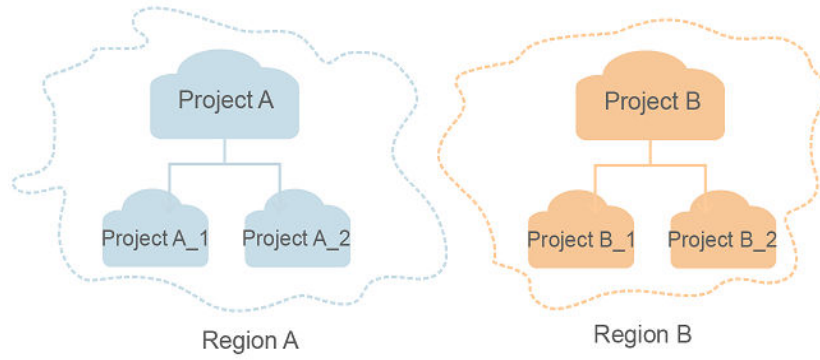
An IAM user is created by an account in IAM to use cloud services. Each IAM user has its own identity credentials (password and access keys).
API authentication requires information such as the account name, username, and password.
- **Region**

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

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

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

Figure 1-1 Project isolation model



2 API Overview

CBR APIs allow you to use all functions provided by CBR.

Table 2-1 API description

Type	Description
Task	Query the task list and the information about a single task.
Vault	Create and query vaults and apply policies to the vaults.
Backup sharing	Share backups with other users. You can perform operations related to backup sharing through this type of APIs.
Restore point	Back up and replicate vaults, and query the time when backups are created.
Backup	Query and synchronize backups, and use backups to restore data.
Policy	Vaults with applied policies can be backed up periodically. You can create, modify, and query policies through policy-related APIs.

3 Calling APIs

3.1 Making an API Request

3.2 Authentication

3.3 Response

3.1 Making an API Request

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

Request URI

A request URI is in the following format:

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

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

Table 3-1 URI parameter description

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

Parameter	Description
query-string	Query parameter, which is optional. Ensure that a question mark (?) is included before each query parameter that is in the format of <i>Parameter name=Parameter value</i> . For example, ?limit=10 indicates that a maximum of 10 data records will be displayed.

 **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.ru-moscow-1 hc.sbercloud.ru/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 <i>Hostname:Port number</i> . If the port number is not specified, the default port is used. The default port number for https is 443 .	No This field is mandatory for AK/SK authentication.	code.test.com or code.test.com:443
Content-Type	Specifies the type (or format) of the message body. The default value application/json is recommended. Other values of this field will be provided for specific APIs if any.	Yes	application/json
Content-Length	Specifies the length of the request body. The unit is byte.	No	3495
X-Project-Id	Specifies the project ID. Obtain the project ID by following the instructions in 7.3 Obtaining a Project ID .	No	e9993fc787d94b6c886cbaa340f9c0f4
X-Auth-Token	Specifies the user token. It is a response to the API for obtaining a user token (This is the only API that does not require authentication). After the request is processed, the value of X-Subject-Token in the response header is the token value.	No This field is mandatory for token authentication.	The following is part of an example token: MIIPAgYJKoZlhvcNAQcCo...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.ru-moscow-1.hc.sbercloud.ru/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 *xxxxxxxxxxxxxxxxxxxx* (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.ru-moscow-1.hc.sbercloud.ru/v3/auth/tokens
Content-Type: application/json
```

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

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.

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

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

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

```
POST https://iam.ru-moscow-1.hc.sbercloud.ru/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 [7.1 Status Codes](#).

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

Response Header

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

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

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

```

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
→ MIIYXQYJKoZIhvcNAQcCoIIYTCCEGEOCAQExDTALBglghkgBZQMEAgEwgharBgkqhkiG9w0BBwGgghacBIIWmHsidG9rZW4iOansiZXhwaXJlc19hdCI6IiwMTktMDItMTNUMC
fj3KJs6YgKnpVNRbW2eZ5eb78SZOkajACgkIQ01wi4JIGzrpd18LGXK5bdfq4lqHCYb8P4NaYONYeJcAgz/VeFYtLWT1GSO0zxKZmlQHq82HBqHdgIZO9fuEbL5dMhdavj+33wEI
xHRCE9I87o+k9-
j+CMZSEB7bUGd5Uj6eRASXl1jipPEGA270g1FruooL6jggIFkNPQuFSOU8+uSsttVwRtnfsC+qTp22Rkd5MCqFGQ8LcuUxC3a+9CMBnOintWW7oeRUUVhVpxk8pxiX1wTEboX-
RzT6MULbvpGw-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 CBR APIs

- [4.1 Tasks](#)
- [4.2 Backup Sharing](#)
- [4.3 Restore Points](#)
- [4.4 Vaults](#)
- [4.5 Backups](#)
- [4.6 Policies](#)

4.1 Tasks

4.1.1 Querying a Single Task

Function

This API is used to query a task by task ID.

URI

GET /v3/{project_id}/operation-logs/{operation_log_id}

Table 4-1 Path Parameters

Parameter	Mandatory	Type	Description
operation_log_id	Yes	String	Task ID
project_id	Yes	String	Project ID

Request Parameters

Table 4-2 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Response Parameters

Status code: 200

Table 4-3 Response body parameters

Parameter	Type	Description
operation_log	OperationLog object	Task information

Table 4-4 OperationLog

Parameter	Type	Description
checkpoint_id	String	Backup record ID
created_at	String	Creation time, for example, 2020-02-23T01:00:32Z
ended_at	String	Task end time, for example, 2020-02-23T01:00:32Z
error_info	OpErrorInfo object	Task error message
extra_info	OpExtraInfo object	Task extension information
id	String	Task ID

Parameter	Type	Description
operation_type	String	Task type Enumeration values: <ul style="list-style-type: none"> • backup • copy • replication • restore • delete • sync • vault_delete • remove_resource
policy_id	String	Policy ID
project_id	String	Project ID
provider_id	String	Backup provider ID, which specifies whether the backup object is a server or disk
started_at	String	Task start time, for example, 2020-02-23T01:00:32Z
status	String	Task status Enumeration values: <ul style="list-style-type: none"> • success • skipped • failed • running • timeout • waiting
updated_at	String	Modification time, for example, 2020-02-23T01:00:32Z
vault_id	String	ID of the vault with which the target resource is associated
vault_name	String	Name of the vault with which the target resource is associated

Table 4-5 OpErrorInfo

Parameter	Type	Description
code	String	For details, see Error Codes .
message	String	Error message

Table 4-6 OpExtralInfo

Parameter	Type	Description
backup	OpExtendInfoBckup object	Extended parameters of backup
common	OpExtendInfoCommon object	Common parameters
delete	OpExtendInfoDelete object	Extended parameters of deletion
sync	OpExtendInfoSync object	Extended parameters of synchronization
remove_resources	OpExtendInfoRemoveResources object	Extended parameters of removing resources from a vault
resource	Resource object	Resource information
restore	OpExtendInfoRestore object	Extended parameters of restoration
vault_delete	OpExtendInfoVaultDelete object	Extended parameters of deleting a vault

Table 4-7 OpExtendInfoBckup

Parameter	Type	Description
backup_id	String	Backup ID
backup_name	String	Backup name
incremental	String	Whether incremental backup is used Enumeration values: <ul style="list-style-type: none"> • "true" • "false"

Table 4-8 OpExtendInfoCommon

Parameter	Type	Description
progress	Integer	Progress of the query task. The value ranges from 0 to 100 . Minimum: 0 Maximum: 100
request_id	String	Request ID
task_id	String	Backup task ID

Table 4-9 OpExtendInfoDelete

Parameter	Type	Description
backup_id	String	Backup ID
backup_name	String	Backup name

Table 4-10 OpExtendInfoSync

Parameter	Type	Description
sync_backup_num	Integer	Number of synchronized backups
delete_backup_num	Integer	Number of deleted backups
err_sync_backup_num	Integer	Number of backups that failed to be synchronized

Table 4-11 OpExtendInfoRemoveResources

Parameter	Type	Description
fail_count	Integer	Number of resources that fail to be deleted
total_count	Integer	Number of deleted backups
resources	Array of Resource objects	Resource information

Table 4-12 Resource

Parameter	Type	Description
id	String	ID of the vault resource type
name	String	Name of the resource to be backed up. The value consists of 0 to 255 characters. Minimum: 0 Maximum: 255
type	String	Type of the resource to be backed up, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo

Table 4-13 ResourceExtraInfo

Parameter	Type	Description
exclude_volumes	Array of strings	IDs of the disks that will not be backed up. This parameter is used when servers are added to a vault, which include all server disks. But some disks do not need to be backed up. Or in case that a server was previously added and some disks on this server do not need to be backed up.

Table 4-14 OpExtendInfoRestore

Parameter	Type	Description
backup_id	String	Backup ID
backup_name	String	Backup name
target_resource_id	String	ID of the resource to be restored
target_resource_name	String	Name of the resource to be restored

Table 4-15 OpExtendInfoVaultDelete

Parameter	Type	Description
fail_count	Integer	Number of resources that fail to be deleted in this task
total_count	Integer	Number of backups deleted in this task

Status code: 404

Table 4-16 Response body parameters

Parameter	Type	Description
error_code	String	For details, see Error Codes .
error_msg	String	Error message

Example Requests

```
GET https://{endpoint}/v3/{project_id}/operation-logs/{operation_log_id}
```

Example Responses

Status code: 200

OK

```
{
  "operation_log" : {
    "status" : "success",
    "provider_id" : "0daac4c5-6707-4851-97ba-169e36266b66",
    "checkpoint_id" : "b432511f-d889-428f-8b0e-5f47c524c6b6",
    "updated_at" : "2019-05-23T14:35:23.584418",
    "error_info" : {
      "message" : "",
      "code" : ""
    },
  },
  "vault_id" : null,
  "started_at" : "2019-05-23T14:31:36.007230",
  "id" : "4827f2da-b008-4507-ab7d-42d0df5ed912",
  "extra_info" : {
    "resource" : {
      "type" : "OS::Nova::Server",
      "id" : "1dab32fa-ebf2-415a-ab0b-eabe6353bc86",
      "name" : "ECS-0001"
    },
  },
  "backup" : {
    "backup_name" : "manualbk_1234",
    "backup_id" : "0e5d0ef6-7f0a-4890-b98c-cb12490e31c1"
  },
  "common" : {
    "progress" : 100,
    "request_id" : "req-cdb98cc4-e87b-4f40-9b4a-57ec036620bc"
  }
},
"ended_at" : "2019-05-23T14:35:23.511155",
"created_at" : "2019-05-23T14:31:36.039365",
"operation_type" : "backup",
"vault_name" : null,
"project_id" : "04f1829c788037ac2fb8c01eb2b04b95",
"policy_id" : null
}
```

Status code: 404

The task ID does not exist.

```
{
  "error_code" : "BackupService.6500",
```

```
"error_msg" : "Operation log does not exist."
}
```

Status Codes

Status Code	Description
200	OK
404	The task ID does not exist.

Error Codes

See [Error Codes](#).

4.1.2 Querying the Task List

Function

This API is used to query the task list.

URI

GET /v3/{project_id}/operation-logs

Table 4-17 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-18 Query Parameters

Parameter	Mandatory	Type	Description
end_time	No	String	End time of a task, in %YYYY-%mm-%ddT%HH:%MM:%SSZ format. For example, 2018-02-01T12:00:00Z .
limit	No	Integer	Number of records displayed per page. The value must be a positive integer. Minimum: 1
offset	No	Integer	Offset value. The value must be a positive integer. Minimum: 1

Parameter	Mandatory	Type	Description
operation_type	No	String	Task type Enumeration values: <ul style="list-style-type: none"> • backup • copy • replication • delete • restore • vault_delete • remove_resource • sync
provider_id	No	String	Backup provider ID, which specifies whether the backup object is a server or disk
resource_id	No	String	Backup resource ID
resource_name	No	String	Backup resource name
start_time	No	String	Start time of a task, in %YYYY-%mm-%ddT%HH:%MM:%SSZ format. For example, 2018-01-01T12:00:00Z .
status	No	String	Task status Enumeration values: <ul style="list-style-type: none"> • success • skipped • failed • running • timeout • waiting
vault_id	No	String	ID of the vault with which the target resource is associated
vault_name	No	String	Name of the vault with which the target resource is associated

Request Parameters

Table 4-19 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Response Parameters

Status code: 200

Table 4-20 Response body parameters

Parameter	Type	Description
operation_logs	Array of OperationLog objects	Task list
count	Integer	Number of tasks
limit	Integer	Number of records displayed on each page Minimum: 1 Maximum: 1000 Default: 1000
offset	Integer	Offset where the query starts Minimum: 0 Default: 0

Table 4-21 OperationLog

Parameter	Type	Description
checkpoint_id	String	Backup record ID
created_at	String	Creation time, for example, 2020-02-23T01:00:32Z
ended_at	String	Task end time, for example, 2020-02-23T01:00:32Z

Parameter	Type	Description
error_info	OpErrorInfo object	Task error message
extra_info	OpExtraInfo object	Task extension information
id	String	Task ID
operation_type	String	Task type Enumeration values: <ul style="list-style-type: none"> • backup • copy • replication • restore • delete • sync • vault_delete • remove_resource
policy_id	String	Policy ID
project_id	String	Project ID
provider_id	String	Backup provider ID, which specifies whether the backup object is a server or disk
started_at	String	Task start time, for example, 2020-02-23T01:00:32Z
status	String	Task status Enumeration values: <ul style="list-style-type: none"> • success • skipped • failed • running • timeout • waiting
updated_at	String	Modification time, for example, 2020-02-23T01:00:32Z
vault_id	String	ID of the vault with which the target resource is associated
vault_name	String	Name of the vault with which the target resource is associated

Table 4-22 OpErrorInfo

Parameter	Type	Description
code	String	For details, see Error Codes .
message	String	Error message

Table 4-23 OpExtralInfo

Parameter	Type	Description
backup	OpExtendInfoBckup object	Extended parameters of backup
common	OpExtendInfoCommon object	Common parameters
delete	OpExtendInfoDelete object	Extended parameters of deletion
sync	OpExtendInfoSync object	Extended parameters of synchronization
remove_resources	OpExtendInfoRemoveResources object	Extended parameters of removing resources from a vault
resource	Resource object	Resource information
restore	OpExtendInfoRestore object	Extended parameters of restoration
vault_delete	OpExtendInfoVaultDelete object	Extended parameters of deleting a vault

Table 4-24 OpExtendInfoBckup

Parameter	Type	Description
backup_id	String	Backup ID
backup_name	String	Backup name

Parameter	Type	Description
incremental	String	Whether incremental backup is used Enumeration values: <ul style="list-style-type: none"> • "true" • "false"

Table 4-25 OpExtendInfoCommon

Parameter	Type	Description
progress	Integer	Progress of the query task. The value ranges from 0 to 100 . Minimum: 0 Maximum: 100
request_id	String	Request ID
task_id	String	Backup task ID

Table 4-26 OpExtendInfoDelete

Parameter	Type	Description
backup_id	String	Backup ID
backup_name	String	Backup name

Table 4-27 OpExtendInfoSync

Parameter	Type	Description
sync_backup_num	Integer	Number of synchronized backups
delete_backup_num	Integer	Number of deleted backups
err_sync_backup_num	Integer	Number of backups that failed to be synchronized

Table 4-28 OpExtendInfoRemoveResources

Parameter	Type	Description
fail_count	Integer	Number of resources that fail to be deleted

Parameter	Type	Description
total_count	Integer	Number of deleted backups
resources	Array of Resource objects	Resource information

Table 4-29 Resource

Parameter	Type	Description
id	String	ID of the vault resource type
name	String	Name of the resource to be backed up. The value consists of 0 to 255 characters. Minimum: 0 Maximum: 255
type	String	Type of the resource to be backed up, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo

Table 4-30 ResourceExtraInfo

Parameter	Type	Description
exclude_volumes	Array of strings	IDs of the disks that will not be backed up. This parameter is used when servers are added to a vault, which include all server disks. But some disks do not need to be backed up. Or in case that a server was previously added and some disks on this server do not need to be backed up.

Table 4-31 OpExtendInfoRestore

Parameter	Type	Description
backup_id	String	Backup ID
backup_name	String	Backup name
target_resource_id	String	ID of the resource to be restored
target_resource_name	String	Name of the resource to be restored

Table 4-32 OpExtendInfoVaultDelete

Parameter	Type	Description
fail_count	Integer	Number of resources that fail to be deleted in this task
total_count	Integer	Number of backups deleted in this task

Status code: 404

Table 4-33 Response body parameters

Parameter	Type	Description
operation_logs	Array of OperationLog objects	Task list
count	Integer	Number of tasks
limit	Integer	Number of records displayed on each page Minimum: 1 Maximum: 1000 Default: 1000
offset	Integer	Offset where the query starts Minimum: 0 Default: 0

Table 4-34 OperationLog

Parameter	Type	Description
checkpoint_id	String	Backup record ID
created_at	String	Creation time, for example, 2020-02-23T01:00:32Z
ended_at	String	Task end time, for example, 2020-02-23T01:00:32Z
error_info	OpErrorInfo object	Task error message
extra_info	OpExtraInfo object	Task extension information
id	String	Task ID

Parameter	Type	Description
operation_type	String	Task type Enumeration values: <ul style="list-style-type: none"> • backup • copy • replication • restore • delete • sync • vault_delete • remove_resource
policy_id	String	Policy ID
project_id	String	Project ID
provider_id	String	Backup provider ID, which specifies whether the backup object is a server or disk
started_at	String	Task start time, for example, 2020-02-23T01:00:32Z
status	String	Task status Enumeration values: <ul style="list-style-type: none"> • success • skipped • failed • running • timeout • waiting
updated_at	String	Modification time, for example, 2020-02-23T01:00:32Z
vault_id	String	ID of the vault with which the target resource is associated
vault_name	String	Name of the vault with which the target resource is associated

Table 4-35 OpErrorInfo

Parameter	Type	Description
code	String	For details, see Error Codes .
message	String	Error message

Table 4-36 OpExtralInfo

Parameter	Type	Description
backup	OpExtendInfoBckup object	Extended parameters of backup
common	OpExtendInfoCommon object	Common parameters
delete	OpExtendInfoDelete object	Extended parameters of deletion
sync	OpExtendInfoSync object	Extended parameters of synchronization
remove_resources	OpExtendInfoRemoveResources object	Extended parameters of removing resources from a vault
resource	Resource object	Resource information
restore	OpExtendInfoRestore object	Extended parameters of restoration
vault_delete	OpExtendInfoVaultDelete object	Extended parameters of deleting a vault

Table 4-37 OpExtendInfoBckup

Parameter	Type	Description
backup_id	String	Backup ID
backup_name	String	Backup name
incremental	String	Whether incremental backup is used Enumeration values: <ul style="list-style-type: none"> • "true" • "false"

Table 4-38 OpExtendInfoCommon

Parameter	Type	Description
progress	Integer	Progress of the query task. The value ranges from 0 to 100 . Minimum: 0 Maximum: 100
request_id	String	Request ID
task_id	String	Backup task ID

Table 4-39 OpExtendInfoDelete

Parameter	Type	Description
backup_id	String	Backup ID
backup_name	String	Backup name

Table 4-40 OpExtendInfoSync

Parameter	Type	Description
sync_backup_num	Integer	Number of synchronized backups
delete_backup_num	Integer	Number of deleted backups
err_sync_backup_num	Integer	Number of backups that failed to be synchronized

Table 4-41 OpExtendInfoRemoveResources

Parameter	Type	Description
fail_count	Integer	Number of resources that fail to be deleted
total_count	Integer	Number of deleted backups
resources	Array of Resource objects	Resource information

Table 4-42 Resource

Parameter	Type	Description
id	String	ID of the vault resource type
name	String	Name of the resource to be backed up. The value consists of 0 to 255 characters. Minimum: 0 Maximum: 255
type	String	Type of the resource to be backed up, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo

Table 4-43 ResourceExtraInfo

Parameter	Type	Description
exclude_volumes	Array of strings	IDs of the disks that will not be backed up. This parameter is used when servers are added to a vault, which include all server disks. But some disks do not need to be backed up. Or in case that a server was previously added and some disks on this server do not need to be backed up.

Table 4-44 OpExtendInfoRestore

Parameter	Type	Description
backup_id	String	Backup ID
backup_name	String	Backup name
target_resource_id	String	ID of the resource to be restored
target_resource_name	String	Name of the resource to be restored

Table 4-45 OpExtendInfoVaultDelete

Parameter	Type	Description
fail_count	Integer	Number of resources that fail to be deleted in this task
total_count	Integer	Number of backups deleted in this task

Example Requests

```
GET https://{endpoint}/v3/{project_id}/operation-logs
```

Example Responses

Status code: 200

OK

```
{
  "count" : 1,
  "operation_logs" : [ {
    "status" : "success",
    "provider_id" : "0daac4c5-6707-4851-97ba-169e36266b66",
    "checkpoint_id" : "b432511f-d889-428f-8b0e-5f47c524c6b6",
    "updated_at" : "2019-05-23T14:35:23.584418",
    "error_info" : {
      "message" : "",
      "code" : ""
    },
    },
    "vault_id" : null,
    "started_at" : "2019-05-23T14:31:36.007230",
    "id" : "4827f2da-b008-4507-ab7d-42d0df5ed912",
    "extra_info" : {
      "resource" : {
        "type" : "OS::Nova::Server",
        "id" : "1dab32fa-ebf2-415a-ab0b-eabe6353bc86",
        "name" : "ECS-0001"
      },
    },
    "backup" : {
      "backup_name" : "manualbk_backup",
      "backup_id" : "0e5d0ef6-7f0a-4890-b98c-cb12490e31c1"
    },
    "common" : {
      "progress" : 100,
      "request_id" : "req-cdb98cc4-e87b-4f40-9b4a-57ec036620bc"
    }
  },
  "ended_at" : "2019-05-23T14:35:23.511155",
  "created_at" : "2019-05-23T14:31:36.039365",
  "operation_type" : "backup",
  "vault_name" : null,
  "project_id" : "04f1829c788037ac2fb8c01eb2b04b95",
  "policy_id" : null
} ] }
```

Status Codes

Status Code	Description
200	OK
404	Not Found

Error Codes

See [Error Codes](#).

4.2 Backup Sharing

4.2.1 Adding a Share Member

Function

This API is used to add a member with whom the backup can be shared. Only cloud server backups can be shared among tenants in the same region.

URI

POST /v3/{project_id}/backups/{backup_id}/members

Table 4-46 Path Parameters

Parameter	Mandatory	Type	Description
backup_id	Yes	String	Backup ID
project_id	Yes	String	Project ID

Request Parameters

Table 4-47 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Table 4-48 Request body parameters

Parameter	Mandatory	Type	Description
members	Yes	Array of strings	Project IDs of the backup share members to be added Array Length: 1 - 10

Response Parameters

Status code: 200

Table 4-49 Response body parameters

Parameter	Type	Description
members	Array of Member objects	Response parameters of adding a backup share member
count	Integer	Number of share members that the backup is shared to

Table 4-50 Member

Parameter	Type	Description
status	String	Backup sharing status Enumeration values: <ul style="list-style-type: none"> • pending • accepted • rejected
created_at	String	Backup sharing time, for example, 2020-02-05T10:38:34.209782
updated_at	String	Update time, for example, 2020-02-05T10:38:34.209782
backup_id	String	Backup ID
image_id	String	ID of the image created by using the accepted shared backup
dest_project_id	String	ID of the project with which the backup is shared
vault_id	String	ID of the vault where the shared backup is stored
id	String	ID of the shared record

Example Requests

Adding members with whom the backup is shared

```
POST https://{endpoint}/v3/0605767b5780d5762fc5c0118072a564/backups/0b07081e-3ec7-4e77-8571-54e2947da422/members
{
  "members" : [ "075e6035d300d48c2fd0c00b78b71ebf" ]
}
```

Example Responses

Status code: 200

OK

```
{
  "members": [ {
    "status": "pending",
    "image_id": null,
    "backup_id": "0b07081e-3ec7-4e77-8571-54e2947da422",
    "vault_id": null,
    "dest_project_id": "075e6035d300d48c2fd0c00b78b71ebf",
    "created_at": "2020-02-05T10:38:34.209782",
    "updated_at": null,
    "id": "3c5a3015-c3a0-4dc6-a1e2-917b90f62319"
  } ]
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.2.2 Updating the Share Member Status

Function

This API is used to update the status of a backup share member.

URI

PUT /v3/{project_id}/backups/{backup_id}/members/{member_id}

Table 4-51 Path Parameters

Parameter	Mandatory	Type	Description
backup_id	Yes	String	Backup ID
member_id	Yes	String	Member ID, which is the same ID as in project ID.
project_id	Yes	String	Project ID

Request Parameters

Table 4-52 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Table 4-53 Request body parameters

Parameter	Mandatory	Type	Description
status	Yes	String	Status of a shared backup Enumeration values: <ul style="list-style-type: none"> • accepted • pending • rejected
vault_id	No	String	Vault in which the shared backup is to be stored. Only UUID is supported. When updating the status of a backup sharing member, if the backup is accepted, vault_id must be specified. If the backup is rejected, vault_id is not required.

Response Parameters

Status code: 200

Table 4-54 Response body parameters

Parameter	Type	Description
member	Member object	Response parameters of querying the details of a backup share member

Table 4-55 Member

Parameter	Type	Description
status	String	Backup sharing status Enumeration values: <ul style="list-style-type: none"> • pending • accepted • rejected
created_at	String	Backup sharing time, for example, 2020-02-05T10:38:34.209782
updated_at	String	Update time, for example, 2020-02-05T10:38:34.209782
backup_id	String	Backup ID
image_id	String	ID of the image created by using the accepted shared backup
dest_project_id	String	ID of the project with which the backup is shared
vault_id	String	ID of the vault where the shared backup is stored
id	String	ID of the shared record

Example Requests

```
PUT https://{endpoint}/v3/f841e01fd2b14e7fa41b6ae7aa6b0594/backups/a5200268-74a5-4806-acc6-95793ab0228b/members/f841e01fd2b14e7fa41b6ae7aa6b0594
```

```
{
  "status": "accepted",
  "vault_id": "4b27c05b-8ad7-48c6-a886-526666c035f0"
}
```

Example Responses

Status code: 200

OK

```
{
  "member": {
    "status": "accepted",
    "image_id": null,
    "backup_id": "17c9acd8-3af3-4401-bab9-ff1cfac15561",
    "vault_id": "4b27c05b-8ad7-48c6-a886-526666c035f0",
    "dest_project_id": "0761021b8900d2622f38c0115db0b331",
    "created_at": "2020-02-24T09:36:00.479033",
    "updated_at": null,
    "id": "824a90b3-c562-448b-ab04-60ea4a97cf60"
  }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.2.3 Querying Share Member Details

Function

This API is used to obtain the details of a backup share member.

URI

GET /v3/{project_id}/backups/{backup_id}/members/{member_id}

Table 4-56 Path Parameters

Parameter	Mandatory	Type	Description
backup_id	Yes	String	Backup ID
member_id	Yes	String	Member ID, which is the project ID of the tenant who receives the shared backup.
project_id	Yes	String	Project ID

Request Parameters

Table 4-57 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Response Parameters

Status code: 200

Table 4-58 Response body parameters

Parameter	Type	Description
member	Member object	Response parameters of querying the details of a backup share member

Table 4-59 Member

Parameter	Type	Description
status	String	Backup sharing status Enumeration values: <ul style="list-style-type: none"> • pending • accepted • rejected
created_at	String	Backup sharing time, for example, 2020-02-05T10:38:34.209782
updated_at	String	Update time, for example, 2020-02-05T10:38:34.209782
backup_id	String	Backup ID
image_id	String	ID of the image created by using the accepted shared backup
dest_project_id	String	ID of the project with which the backup is shared
vault_id	String	ID of the vault where the shared backup is stored
id	String	ID of the shared record

Example Requests

GET https://{endpoint}/v3/{project_id}/backups/{backup_id}/members/{member_id}

Example Responses

Status code: 200

OK

```
{
  "member": {
    "status": "accepted",
```

```

"image_id" : null,
"backup_id" : "17c9acd8-3af3-4401-bab9-ff1cfac15561",
"vault_id" : "4b27c05b-8ad7-48c6-a886-526666c035f0",
"dest_project_id" : "0761021b8900d2622f38c0115db0b331",
"created_at" : "2020-02-24T09:36:00.479033",
"updated_at" : null,
"id" : "824a90b3-c562-448b-ab04-60ea4a97cf60"
}
}

```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.2.4 Obtaining the Share Member List

Function

This API is used to obtain the list of backup share members.

URI

GET /v3/{project_id}/backups/{backup_id}/members

Table 4-60 Path Parameters

Parameter	Mandatory	Type	Description
backup_id	Yes	String	Backup ID
project_id	Yes	String	Project ID

Table 4-61 Query Parameters

Parameter	Mandatory	Type	Description
dest_project_id	No	String	ID of the project with which the backup is shared
image_id	No	String	ID of the image created from the accepted backup
limit	No	Integer	Number of records displayed per page. The value must be a positive integer.

Parameter	Mandatory	Type	Description
marker	No	String	ID of the last record displayed on the previous page. Only UUID is supported.
offset	No	Integer	Offset value, which is a positive integer.
sort	No	String	A group of properties separated by commas (,) and sorting directions. The value is in the format of <key1>[:<direction>],<key2>[:<direction>], where the value of direction is asc (ascending order) or desc (descending order). If a direction is not specified, the default sorting direction is desc . The value of sort can contain a maximum of 255 characters.
status	No	String	Status of a shared backup
vault_id	No	String	ID of the vault where the shared backup is stored. Only UUID is supported.

Request Parameters

Table 4-62 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Response Parameters

Status code: 200

Table 4-63 Response body parameters

Parameter	Type	Description
members	Array of Member objects	Response parameters of adding a backup share member
count	Integer	Number of share members that the backup is shared to

Table 4-64 Member

Parameter	Type	Description
status	String	Backup sharing status Enumeration values: <ul style="list-style-type: none"> • pending • accepted • rejected
created_at	String	Backup sharing time, for example, 2020-02-05T10:38:34.209782
updated_at	String	Update time, for example, 2020-02-05T10:38:34.209782
backup_id	String	Backup ID
image_id	String	ID of the image created by using the accepted shared backup
dest_project_id	String	ID of the project with which the backup is shared
vault_id	String	ID of the vault where the shared backup is stored
id	String	ID of the shared record

Example Requests

```
GET https://{endpoint}/v3/{project_id}/backups/{backup_id}/members
```

Example Responses

Status code: 200

OK

```
{
  "members": [ {
    "status": "pending",
    "image_id": null,
```

```

"backup_id" : "0b07081e-3ec7-4e77-8571-54e2947da422",
"vault_id" : null,
"dest_project_id" : "075e6035d300d48c2fd0c00b78b71ebf",
"created_at" : "2020-02-05T10:38:34.209782",
"updated_at" : null,
"id" : "3c5a3015-c3a0-4dc6-a1e2-917b90f62319"
}],
"count" : 50
}

```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.2.5 Deleting a Specified Share Member

Function

This API is used to delete a specified backup share member.

URI

DELETE /v3/{project_id}/backups/{backup_id}/members/{member_id}

Table 4-65 Path Parameters

Parameter	Mandatory	Type	Description
backup_id	Yes	String	Backup ID
member_id	Yes	String	Member ID, which is the same ID as in project ID.
project_id	Yes	String	Project ID

Request Parameters

Table 4-66 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Response Parameters

None

Example Requests

```
DELETE https://{endpoint}/v3/{project_id}/backups/{backup_id}/members/{member_id}
```

Example Responses

None

Status Codes

Status Code	Description
204	No Content

Error Codes

See [Error Codes](#).

4.3 Restore Points

4.3.1 Querying a Restore Point

Function

This API is used to query a specified restore point based on its ID.

URI

```
GET /v3/{project_id}/checkpoints/{checkpoint_id}
```

Table 4-67 Path Parameters

Parameter	Mandatory	Type	Description
checkpoint_id	Yes	String	Restore point ID
project_id	Yes	String	Project ID

Request Parameters

Table 4-68 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Response Parameters

Status code: 200

Table 4-69 Response body parameters

Parameter	Type	Description
checkpoint	CheckpointCreate object	Restore point information

Table 4-70 CheckpointCreate

Parameter	Type	Description
created_at	String	Creation time, for example, 2020-02-05T10:38:34.209782
id	String	Restore point ID
project_id	String	Project ID

Parameter	Type	Description
status	String	Status Enumeration values: <ul style="list-style-type: none"> • available • deleting • protecting • deleted • error-deleting • error
vault	CheckpointPlanCreate object	Vault information
extra_info	CheckpointExtraInfoResp object	Extended information

Table 4-71 CheckpointPlanCreate

Parameter	Type	Description
id	String	Vault ID
name	String	Vault name
resources	Array of CheckpointResourceResp objects	Backup objects
skipped_resources	Array of CheckpointCreateSkippedResource objects	Resources skipped during backup

Table 4-72 CheckpointResourceResp

Parameter	Type	Description
extra_info	String	Extra information of the resource
id	String	ID of the resource to be backed up
name	String	Name of the resource to be backed up

Parameter	Type	Description
protect_status	String	Protected status Enumeration values: <ul style="list-style-type: none"> • available • error • protecting • restoring • removing
resource_size	String	Allocated capacity for the associated resource, in GB
type	String	Type of the resource to be backed up, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo
backup_size	String	Backup size
backup_count	String	Number of backups

Table 4-73 CheckpointCreateSkippedResource

Parameter	Type	Description
id	String	Resource ID
type	String	Resource type
name	String	Resource name
code	String	For details, see Error Codes .
reason	String	Reason for the skipping. For example, the resource is being backed up.

Table 4-74 CheckpointExtraInfoResp

Parameter	Type	Description
name	String	Backup name
description	String	Backup description
retention_duration	Integer	Number of days that backups can be retained

Example Requests

```
GET https://{endpoint}/v3/4229d7a45436489f8c3dc2b1d35d4987/checkpoints/8b0851a8-adf3-4f4c-a914-dead08bf9664
```

Example Responses

Status code: 200

OK

```
{
  "checkpoint" : {
    "status" : "available",
    "created_at" : "2019-05-10T07:59:12.036982",
    "vault" : {
      "id" : "3b5816b5-f29c-4172-9d9a-76c719a659ce",
      "resources" : [ {
        "name" : "ecs-1f0f-0002",
        "resource_size" : "40",
        "protect_status" : "available",
        "type" : "OS::Nova::Server",
        "id" : "94eba8b2-acc9-4d82-badc-127144cc5526",
        "extra_info" : null
      } ],
      "name" : "vault-be94"
    },
    "project_id" : "4229d7a45436489f8c3dc2b1d35d4987",
    "id" : "8b0851a8-adf3-4f4c-a914-dead08bf9664",
    "extra_info" : null
  }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.3.2 Creating a Restore Point

Function

This API is used to back up a vault and generate a restore point.

URI

POST /v3/{project_id}/checkpoints

Table 4-75 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-76 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Table 4-77 Request body parameters

Parameter	Mandatory	Type	Description
checkpoint	Yes	VaultBackup object	Parameters for backing up the vault

Table 4-78 VaultBackup

Parameter	Mandatory	Type	Description
parameters	No	CheckpointParam object	Parameters
vault_id	Yes	String	Vault ID

Table 4-79 CheckpointParam

Parameter	Mandatory	Type	Description
auto_trigger	No	Boolean	Whether automatic triggering is enabled. Possible values are true (yes) and false (no). Default: false
description	No	String	Backup description Minimum: 0 Maximum: 255

Parameter	Mandatory	Type	Description
incremental	No	Boolean	Whether the backup is an incremental backup. Possible values are true (yes) and false (no). Default: true
name	No	String	Backup name, which can contain only digits, letters, underscores (_), and hyphens (-) Minimum: 1 Maximum: 64
resources	No	Array of strings	UUID list of resources to be backed up
resource_details	No	Array of Resource objects	Resource details Array Length: 0 - 256

Table 4-80 Resource

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the vault resource type
name	No	String	Name of the resource to be backed up. The value consists of 0 to 255 characters. Minimum: 0 Maximum: 255
type	Yes	String	Type of the resource to be backed up, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo

Table 4-81 ResourceExtraInfo

Parameter	Mandatory	Type	Description
exclude_volumes	No	Array of strings	IDs of the disks that will not be backed up. This parameter is used when servers are added to a vault, which include all server disks. But some disks do not need to be backed up. Or in case that a server was previously added and some disks on this server do not need to be backed up.

Response Parameters

Status code: 200

Table 4-82 Response body parameters

Parameter	Type	Description
checkpoint	CheckpointCreate object	Restore point information

Table 4-83 CheckpointCreate

Parameter	Type	Description
created_at	String	Creation time, for example, 2020-02-05T10:38:34.209782
id	String	Restore point ID
project_id	String	Project ID
status	String	Status Enumeration values: <ul style="list-style-type: none"> • available • deleting • protecting • deleted • error-deleting • error
vault	CheckpointPlanCreate object	Vault information

Parameter	Type	Description
extra_info	CheckpointExtraInfoResp object	Extended information

Table 4-84 CheckpointPlanCreate

Parameter	Type	Description
id	String	Vault ID
name	String	Vault name
resources	Array of CheckpointResourceResp objects	Backup objects
skipped_resources	Array of CheckpointCreateSkippedResource objects	Resources skipped during backup

Table 4-85 CheckpointResourceResp

Parameter	Type	Description
extra_info	String	Extra information of the resource
id	String	ID of the resource to be backed up
name	String	Name of the resource to be backed up
protect_status	String	Protected status Enumeration values: <ul style="list-style-type: none"> • available • error • protecting • restoring • removing
resource_size	String	Allocated capacity for the associated resource, in GB
type	String	Type of the resource to be backed up, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo

Parameter	Type	Description
backup_size	String	Backup size
backup_count	String	Number of backups

Table 4-86 CheckpointCreateSkippedResource

Parameter	Type	Description
id	String	Resource ID
type	String	Resource type
name	String	Resource name
code	String	For details, see Error Codes .
reason	String	Reason for the skipping. For example, the resource is being backed up.

Table 4-87 CheckpointExtraInfoResp

Parameter	Type	Description
name	String	Backup name
description	String	Backup description
retention_duration	Integer	Number of days that backups can be retained

Example Requests

Automatically backing up a vault and generating a restore point

POST https://{endpoint}/v3/f841e01fd2b14e7fa41b6ae7aa6b0594/checkpoints

```
{
  "checkpoint": {
    "parameters": {
      "auto_trigger": true,
      "description": "backup_description",
      "incremental": true,
      "name": "backup_name",
      "resources": [ "94eba8b2-acc9-4d82-badc-127144cc5526" ]
    },
    "vault_id": "3b5816b5-f29c-4172-9d9a-76c719a659ce"
  }
}
```

Example Responses

Status code: 200

OK

```
{
  "checkpoint" : {
    "status" : "protecting",
    "created_at" : "2019-05-10T07:59:12.733403",
    "vault" : {
      "skipped_resources" : [ ],
      "id" : "3b5816b5-f29c-4172-9d9a-76c719a659ce",
      "resources" : [ {
        "name" : "ecs-1f0f-0002",
        "resource_size" : "40",
        "protect_status" : "available",
        "type" : "OS::Nova::Server",
        "id" : "94eba8b2-acc9-4d82-badc-127144cc5526",
        "extra_info" : null
      } ],
      "name" : "vault-be94"
    },
    "project_id" : "4229d7a45436489f8c3dc2b1d35d4987",
    "id" : "8b0851a8-adf3-4f4c-a914-dead08bf9664",
    "extra_info" : {
      "retention_duration" : -1,
      "name" : "backup_name",
      "description" : "backup_description"
    }
  }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.4 Vaults

4.4.1 Creating a Vault

Function

This API is used to create a vault.

URI

POST /v3/{project_id}/vaults

Table 4-88 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-89 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Table 4-90 Request body parameters

Parameter	Mandatory	Type	Description
vault	Yes	VaultCreate object	Parameters for creating a vault

Table 4-91 VaultCreate

Parameter	Mandatory	Type	Description
backup_policy_id	No	String	Backup policy ID. If the value of this parameter is null, automatic backup is not performed.
billing	Yes	BillingCreate object	Parameter information for creation
description	No	String	User-defined vault description Minimum: 0 Maximum: 64
name	Yes	String	Vault name Minimum: 1 Maximum: 64

Parameter	Mandatory	Type	Description
resources	Yes	Array of ResourceCreate objects	Associated resources. Set this parameter to [] if no resources are associated when creating a vault. Array Length: 0 - 255
tags	No	Array of Tag objects	Tag list It cannot be an empty list. The list can contain up to 10 keys. Keys in this list must be unique.
auto_bind	No	Boolean	Whether automatic association is supported
bind_rules	No	VaultBindRules object	Rules for automatic association
backup_name_prefix	No	String	Backup name prefix. If configured, the names of all automatic backups generated for the vault will use this prefix. Minimum: 0 Maximum: 32

Table 4-92 BillingCreate

Parameter	Mandatory	Type	Description
cloud_type	No	String	Cloud type, which is public
consistent_level	Yes	String	Vault specification, which is crash_consistent by default (crash consistent backup)
object_type	Yes	String	Object type, which can be server, disk, or turbo
protect_type	Yes	String	Protection type, which is backup
size	Yes	Integer	Capacity, in GB Minimum: 10 Maximum: 10485760
charging_mode	No	String	Billing mode, which is post_paid Default: post_paid

Parameter	Mandatory	Type	Description
is_auto_renew	No	Boolean	Whether to automatically renew the subscription after expiration. By default, it is not renewed. Default: false
is_auto_pay	No	Boolean	Whether the fee is automatically deducted from the customer's account balance after an order is submitted. The non-automatic payment mode is used by default. Default: false
console_url	No	String	Redirection URL Minimum: 1 Maximum: 255
is_multi_az	No	Boolean	Multi-AZ attribute of a vault. The default value is false . Default: false

Table 4-93 ResourceCreate

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the resource to be backed up
type	Yes	String	Type of the resource to be backed up, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo
name	No	String	Resource name Minimum: 0 Maximum: 255

Table 4-94 ResourceExtraInfo

Parameter	Mandatory	Type	Description
exclude_volumes	No	Array of strings	IDs of the disks that will not be backed up. This parameter is used when servers are added to a vault, which include all server disks. But some disks do not need to be backed up. Or in case that a server was previously added and some disks on this server do not need to be backed up.

Table 4-95 Tag

Parameter	Mandatory	Type	Description
key	Yes	String	<p>Key</p> <p>It can contain a maximum of 36 characters.</p> <p>It cannot be an empty string.</p> <p>Spaces before and after a key will be discarded.</p> <p>It cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, /</p> <p>It can contain only letters, digits, hyphens (-), and underscores (_).</p>

Parameter	Mandatory	Type	Description
value	Yes	String	<p>Value</p> <p>It is mandatory when a tag is added and optional when a tag is deleted.</p> <p>It can contain a maximum of 43 characters.</p> <p>It can be an empty string. Spaces before and after a value will be discarded.</p> <p>It cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, /</p> <p>It can contain only letters, digits, hyphens (-), and underscores (_).</p>

Table 4-96 VaultBindRules

Parameter	Mandatory	Type	Description
tags	No	Array of BindRulesTags objects	<p>Filters automatically associated resources by tag.</p> <p>Minimum length: 0 characters</p> <p>Maximum length: 5 characters</p> <p>Array Length: 0 - 5</p>

Table 4-97 BindRulesTags

Parameter	Mandatory	Type	Description
key	Yes	String	<p>The key cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, /</p> <p>The key can contain only letters, digits, underscores (_), and hyphens (-).</p>

Parameter	Mandatory	Type	Description
value	Yes	String	The value cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, / The value can contain only letters, digits, underscores (_), and hyphens (-).

Response Parameters

Status code: 200

Table 4-98 Response body parameters

Parameter	Type	Description
vault	VaultCreateResource object	Objects returned after a vault query

Table 4-99 VaultCreateResource

Parameter	Type	Description
billing	Billing object	Operations information
description	String	User-defined vault description Minimum: 0 Maximum: 255
id	String	Vault ID
name	String	Vault name Minimum: 1 Maximum: 64
project_id	String	Project ID
provider_id	String	ID of the vault resource type
resources	Array of ResourceRes p objects	Vault resources
tags	Array of Tag objects	Vault tags

Parameter	Type	Description
auto_bind	Boolean	Whether to enable automatic association. Its default value is false (not enable).
bind_rules	VaultBindRules object	Association rules
user_id	String	User ID
created_at	String	Creation time, for example, 2020-02-05T10:38:34.209782
auto_expand	Boolean	Whether to enable auto capacity expansion for the vault.
backup_name_prefix	String	Backup name prefix Minimum: 0 Maximum: 32
demand_billing	Boolean	Whether the vault capacity can be exceeded. Default: false
cbc_delete_count	Integer	Vault deletion count Default: 0
frozen	Boolean	Whether the vault is frozen Default: false

Table 4-100 Billing

Parameter	Type	Description
allocated	Integer	Allocated capacity, in GB.
charging_mode	String	Billing mode, which is post_paid
cloud_type	String	Cloud type, which is public
consistent_level	String	Vault specification, which is crash_consistent by default (crash consistent backup)
object_type	String	Object type, which can be server , disk , or turbo
order_id	String	Order ID
product_id	String	Product ID
protect_type	String	Protection type, which is backup

Parameter	Type	Description
size	Integer	Capacity, in GB Minimum: 1 Maximum: 10485760
spec_code	String	Specification code Server backup vault: vault.backup.server.normal ; Disk backup vault: vault.backup.volume.normal ; File system backup vault: vault.backup.turbo.normal
status	String	Vault status Enumeration values: <ul style="list-style-type: none"> • available • lock • frozen • deleting • error
storage_unit	String	Name of the bucket for the vault
used	Integer	Used capacity, in MB.
frozen_scene	String	Scenario when an account is frozen
is_multi_az	Boolean	Multi-AZ attribute of a vault Default: false

Table 4-101 ResourceResp

Parameter	Type	Description
id	String	ID of the resource to be backed up
name	String	Name of the resource to be backed up Minimum: 0 Maximum: 255
protect_status	String	Protection status Enumeration values: <ul style="list-style-type: none"> • available • error • protecting • restoring • removing

Parameter	Type	Description
size	Integer	Allocated capacity for the associated resources, in GB
type	String	Type of the resource to be backed up, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo
backup_size	Integer	Backup size
backup_count	Integer	Number of backups

Table 4-102 ResourceExtraInfo

Parameter	Type	Description
exclude_volumes	Array of strings	IDs of the disks that will not be backed up. This parameter is used when servers are added to a vault, which include all server disks. But some disks do not need to be backed up. Or in case that a server was previously added and some disks on this server do not need to be backed up.

Table 4-103 Tag

Parameter	Type	Description
key	String	Key It can contain a maximum of 36 characters. It cannot be an empty string. Spaces before and after a key will be discarded. It cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, / It can contain only letters, digits, hyphens (-), and underscores (_).

Parameter	Type	Description
value	String	<p>Value</p> <p>It is mandatory when a tag is added and optional when a tag is deleted.</p> <p>It can contain a maximum of 43 characters.</p> <p>It can be an empty string.</p> <p>Spaces before and after a value will be discarded.</p> <p>It cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, /</p> <p>It can contain only letters, digits, hyphens (-), and underscores (_).</p>

Table 4-104 VaultBindRules

Parameter	Type	Description
tags	Array of BindRulesTags objects	<p>Filters automatically associated resources by tag.</p> <p>Minimum length: 0 characters</p> <p>Maximum length: 5 characters</p> <p>Array Length: 0 - 5</p>

Table 4-105 BindRulesTags

Parameter	Type	Description
key	String	<p>The key cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, /</p> <p>The key can contain only letters, digits, underscores (_), and hyphens (-).</p>
value	String	<p>The value cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, /</p> <p>The value can contain only letters, digits, underscores (_), and hyphens (-).</p>

Status code: 400

Table 4-106 Response body parameters

Parameter	Type	Description
error_code	String	For details, see Error Codes .
error_msg	String	Error message

Example Requests

- Creating a 100-GB pay-per-use cloud server backup vault, associating resources, and adding tags

```
POST https://{endpoint}/v3/f841e01fd2b14e7fa41b6ae7aa6b0594/vaults
{
  "vault": {
    "backup_policy_id": "6dd81d7d-a4cb-443e-b8ed-1af0bd3a261b",
    "billing": {
      "cloud_type": "public",
      "consistent_level": "crash_consistent",
      "object_type": "server",
      "protect_type": "backup",
      "size": 100,
      "charging_mode": "post_paid",
      "is_auto_renew": false,
      "is_auto_pay": false,
      "console_url": "https://console.demo.com/cbr/?agencyId=97fcd896b7914cb98f553a087232e243&region=testregion/cbr/manager/csbs/vaultList"
    },
    "description": "vault_description",
    "name": "vault_name",
    "resources": [ {
      "extra_info": {
        "exclude_volumes": [ "43a320a5-3efd-4568-b1aa-8dd9183cc64b" ]
      },
      "id": "23a320a5-3efd-4568-b1aa-8dd9183cc64c",
      "type": "OS::Nova::Server"
    } ],
    "tags": [ {
      "key": "key01",
      "value": "value01"
    } ],
    "enterprise_project_id": "0"
  }
}
```

- Creating a 40-GB pay-per-use cloud disk backup vault

```
POST https://{endpoint}/v3/f841e01fd2b14e7fa41b6ae7aa6b0594/vaults
{
  "vault": {
    "billing": {
      "consistent_level": "crash_consistent",
      "object_type": "disk",
      "protect_type": "backup",
      "size": 40,
      "charging_mode": "post_paid",
      "is_auto_renew": false,
      "is_auto_pay": false
    },
    "name": "test",
    "resources": [ ]
  }
}
```

Example Responses

Status code: 200

OK

```
{
  "vault" : {
    "provider_id" : "0daac4c5-6707-4851-97ba-169e36266b66",
    "description" : "vault_description",
    "tags" : [ {
      "value" : "value01",
      "key" : "key01"
    } ],
    "enterprise_project_id" : "0",
    "auto_bind" : false,
    "id" : "ad7627ae-5b0b-492e-b6bd-cd809b745197",
    "user_id" : "38d65be2ecd840d19046e239e841a734",
    "name" : "vault_name",
    "billing" : {
      "status" : "available",
      "used" : 0,
      "protect_type" : "backup",
      "order_id" : null,
      "object_type" : "server",
      "allocated" : 40,
      "spec_code" : "vault.backup.server.normal",
      "size" : 100,
      "cloud_type" : "public",
      "product_id" : null,
      "consistent_level" : "crash_consistent",
      "storage_unit" : null,
      "charging_mode" : "post_paid"
    },
    "created_at" : "2019-05-23T12:51:10.071232",
    "project_id" : "fc347bc64ccd4589ae52e4f44b7433c7",
    "resources" : [ {
      "name" : "ecs-b977-0002",
      "backup_size" : 0,
      "protect_status" : "available",
      "backup_count" : 0,
      "extra_info" : {
        "exclude_volumes" : [ "1855eb9a-2b5e-4938-a9f0-aea08b6f9243", "5a51e8b3-2f65-4045-896f-f8ffae14b064" ]
      },
      "type" : "OS::Nova::Server",
      "id" : "23a320a5-3efd-4568-b1aa-8dd9183cc64c",
      "size" : 40
    } ]
  }
}
```

Status Codes

Status Code	Description
200	OK
400	Bad Request

Error Codes

See [Error Codes](#).

4.4.2 Querying a Specified Vault

Function

This API is used to query a specified vault based on its ID.

URI

GET /v3/{project_id}/vaults/{vault_id}

Table 4-107 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
vault_id	Yes	String	Vault ID

Request Parameters

Table 4-108 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Response Parameters

Status code: 200

Table 4-109 Response body parameters

Parameter	Type	Description
vault	Vault object	Objects returned after the query by a vault

Table 4-110 Vault

Parameter	Type	Description
billing	Billing object	Operation info

Parameter	Type	Description
description	String	User-defined vault description Minimum: 0 Maximum: 255
id	String	Vault ID
name	String	Vault name Minimum: 1 Maximum: 64
project_id	String	Project ID
provider_id	String	ID of the vault resource type
resources	Array of ResourceRes p objects	Vault resources
tags	Array of Tag objects	Vault tags
auto_bind	Boolean	Indicates whether automatic association is enabled. Its default value is false (not enabled).
bind_rules	VaultBindRul es object	Association rule
user_id	String	User ID
created_at	String	Creation time, for example, 2020-02-05T10:38:34.209782
auto_expand	Boolean	Whether to enable auto capacity expansion for the vault.

Table 4-111 Billing

Parameter	Type	Description
allocated	Integer	Allocated capacity, in GB.
charging_mode	String	Billing mode, which is post_paid
cloud_type	String	Cloud type, which is public
consistent_level	String	Vault specification, which is crash_consistent by default (crash consistent backup)
object_type	String	Object type, which can be server , disk , or turbo

Parameter	Type	Description
order_id	String	Order ID
product_id	String	Product ID
protect_type	String	Protection type, which is backup
size	Integer	Capacity, in GB Minimum: 1 Maximum: 10485760
spec_code	String	Specification code Server backup vault: vault.backup.server.normal ; Disk backup vault: vault.backup.volume.normal ; File system backup vault: vault.backup.turbo.normal
status	String	Vault status Enumeration values: <ul style="list-style-type: none"> • available • lock • frozen • deleting • error
storage_unit	String	Name of the bucket for the vault
used	Integer	Used capacity, in MB.
frozen_scene	String	Scenario when an account is frozen
is_multi_az	Boolean	Multi-AZ attribute of a vault Default: false

Table 4-112 ResourceResp

Parameter	Type	Description
id	String	ID of the resource to be backed up
name	String	Name of the resource to be backed up Minimum: 0 Maximum: 255

Parameter	Type	Description
protect_status	String	Protection status Enumeration values: <ul style="list-style-type: none"> • available • error • protecting • restoring • removing
size	Integer	Allocated capacity for the associated resources, in GB
type	String	Type of the resource to be backed up, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo
backup_size	Integer	Backup size
backup_count	Integer	Number of backups

Table 4-113 ResourceExtraInfo

Parameter	Type	Description
exclude_volumes	Array of strings	IDs of the disks that will not be backed up. This parameter is used when servers are added to a vault, which include all server disks. But some disks do not need to be backed up. Or in case that a server was previously added and some disks on this server do not need to be backed up.

Table 4-114 Tag

Parameter	Type	Description
key	String	Key It can contain a maximum of 36 characters. It cannot be an empty string. Spaces before and after a key will be discarded. It cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, / It can contain only letters, digits, hyphens (-), and underscores (_).

Parameter	Type	Description
value	String	<p>Value</p> <p>It is mandatory when a tag is added and optional when a tag is deleted.</p> <p>It can contain a maximum of 43 characters.</p> <p>It can be an empty string.</p> <p>Spaces before and after a value will be discarded.</p> <p>It cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, /</p> <p>It can contain only letters, digits, hyphens (-), and underscores (_).</p>

Table 4-115 VaultBindRules

Parameter	Type	Description
tags	Array of BindRulesTags objects	<p>Filters automatically associated resources by tag.</p> <p>Minimum length: 0 characters</p> <p>Maximum length: 5 characters</p> <p>Array Length: 0 - 5</p>

Table 4-116 BindRulesTags

Parameter	Type	Description
key	String	<p>The key cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, /</p> <p>The key can contain only letters, digits, underscores (_), and hyphens (-).</p>
value	String	<p>The value cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, /</p> <p>The value can contain only letters, digits, underscores (_), and hyphens (-).</p>

Status code: 404

Table 4-117 Response body parameters

Parameter	Type	Description
vault	Vault object	Objects returned after the query by a vault

Table 4-118 Vault

Parameter	Type	Description
billing	Billing object	Operation info
description	String	User-defined vault description Minimum: 0 Maximum: 255
id	String	Vault ID
name	String	Vault name Minimum: 1 Maximum: 64
project_id	String	Project ID
provider_id	String	ID of the vault resource type
resources	Array of ResourceRes p objects	Vault resources
tags	Array of Tag objects	Vault tags
auto_bind	Boolean	Indicates whether automatic association is enabled. Its default value is false (not enabled).
bind_rules	VaultBindRul es object	Association rule
user_id	String	User ID
created_at	String	Creation time, for example, 2020-02-05T10:38:34.209782
auto_expand	Boolean	Whether to enable auto capacity expansion for the vault.

Table 4-119 Billing

Parameter	Type	Description
allocated	Integer	Allocated capacity, in GB.
charging_mode	String	Billing mode, which is post_paid
cloud_type	String	Cloud type, which is public
consistent_level	String	Vault specification, which is crash_consistent by default (crash consistent backup)
object_type	String	Object type, which can be server , disk , or turbo
order_id	String	Order ID
product_id	String	Product ID
protect_type	String	Protection type, which is backup
size	Integer	Capacity, in GB Minimum: 1 Maximum: 10485760
spec_code	String	Specification code Server backup vault: vault.backup.server.normal ; Disk backup vault: vault.backup.volume.normal ; File system backup vault: vault.backup.turbo.normal
status	String	Vault status Enumeration values: <ul style="list-style-type: none"> • available • lock • frozen • deleting • error
storage_unit	String	Name of the bucket for the vault
used	Integer	Used capacity, in MB.
frozen_scene	String	Scenario when an account is frozen
is_multi_az	Boolean	Multi-AZ attribute of a vault Default: false

Table 4-120 ResourceResp

Parameter	Type	Description
id	String	ID of the resource to be backed up
name	String	Name of the resource to be backed up Minimum: 0 Maximum: 255
protect_status	String	Protection status Enumeration values: <ul style="list-style-type: none"> • available • error • protecting • restoring • removing
size	Integer	Allocated capacity for the associated resources, in GB
type	String	Type of the resource to be backed up, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo
backup_size	Integer	Backup size
backup_count	Integer	Number of backups

Table 4-121 ResourceExtraInfo

Parameter	Type	Description
exclude_volumes	Array of strings	IDs of the disks that will not be backed up. This parameter is used when servers are added to a vault, which include all server disks. But some disks do not need to be backed up. Or in case that a server was previously added and some disks on this server do not need to be backed up.

Table 4-122 Tag

Parameter	Type	Description
key	String	<p>Key</p> <p>It can contain a maximum of 36 characters.</p> <p>It cannot be an empty string.</p> <p>Spaces before and after a key will be discarded.</p> <p>It cannot contain non-printable ASCII characters (0–31) and the following characters: =*<>, /</p> <p>It can contain only letters, digits, hyphens (-), and underscores (_).</p>
value	String	<p>Value</p> <p>It is mandatory when a tag is added and optional when a tag is deleted.</p> <p>It can contain a maximum of 43 characters.</p> <p>It can be an empty string.</p> <p>Spaces before and after a value will be discarded.</p> <p>It cannot contain non-printable ASCII characters (0–31) and the following characters: =*<>, /</p> <p>It can contain only letters, digits, hyphens (-), and underscores (_).</p>

Table 4-123 VaultBindRules

Parameter	Type	Description
tags	Array of BindRulesTags objects	<p>Filters automatically associated resources by tag.</p> <p>Minimum length: 0 characters</p> <p>Maximum length: 5 characters</p> <p>Array Length: 0 - 5</p>

Table 4-124 BindRulesTags

Parameter	Type	Description
key	String	The key cannot contain non-printable ASCII characters (0–31) and the following characters: =*<>, / The key can contain only letters, digits, underscores (_), and hyphens (-).
value	String	The value cannot contain non-printable ASCII characters (0–31) and the following characters: =*<>, / The value can contain only letters, digits, underscores (_), and hyphens (-).

Example Requests

Querying a vault

```
GET https://{endpoint}/v3/{project_id}/vaults/{vault_id}
```

Example Responses

Status code: 200

OK

```
{
  "vault": {
    "id": "2b076f26-391f-40fa-bf71-a798940faccf",
    "name": "sdk-vault1595581958",
    "description": null,
    "resources": [ ],
    "provider_id": "0daac4c5-6707-4851-97ba-169e36266b66",
    "created_at": "2020-07-24T09:12:49.491874",
    "project_id": "0605767b5780d5762fc5c0118072a564",
    "enterprise_project_id": "0",
    "auto_bind": true,
    "bind_rules": { },
    "auto_expand": false,
    "user_id": "aa2999fa5ae640f28926f8fd79188934",
    "billing": {
      "allocated": 0,
      "cloud_type": "public",
      "consistent_level": "crash_consistent",
      "frozen_scene": null,
      "charging_mode": "post_paid",
      "order_id": null,
      "product_id": null,
      "protect_type": "backup",
      "object_type": "server",
      "spec_code": "vault.backup.server.normal",
      "used": 0,
      "storage_unit": null,
      "status": "available",
      "size": 40
    },
    "tags": [ {
      "key": "fds",
      "value": null
    } ]
  }
}
```

```
    }}
  }
}
```

Status Codes

Status Code	Description
200	OK
404	Not Found

Error Codes

See [Error Codes](#).

4.4.3 Querying the Vault List

Function

This API is used to query the vault list.

URI

GET /v3/{project_id}/vaults

Table 4-125 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-126 Query Parameters

Parameter	Mandatory	Type	Description
cloud_type	No	String	Cloud type, which is public
id	No	String	Vault ID
limit	No	Integer	Number of records displayed per page. The value must be a positive integer. Minimum: 1 Maximum: 1000
name	No	String	Vault name

Parameter	Mandatory	Type	Description
object_type	No	String	Object type, which can be server , disk , or turbo
offset	No	Integer	Offset value. The value must be a positive integer.
policy_id	No	String	Policy ID
protect_type	No	String	Protection type, which is backup
resource_ids	No	String	Resource ID. Multiple resources are separated with commas (,).
status	No	String	Status

Request Parameters

Table 4-127 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Response Parameters

Status code: 200

Table 4-128 Response body parameters

Parameter	Type	Description
vaults	Array of Vault objects	Vault instance list
count	Integer	Number of vaults
limit	Integer	Number of records displayed on each page Minimum: 1 Maximum: 1000 Default: 1000

Parameter	Type	Description
offset	Integer	Offset where the query starts Minimum: 0 Default: 0

Table 4-129 Vault

Parameter	Type	Description
billing	Billing object	Operation info
description	String	User-defined vault description Minimum: 0 Maximum: 255
id	String	Vault ID
name	String	Vault name Minimum: 1 Maximum: 64
project_id	String	Project ID
provider_id	String	ID of the vault resource type
resources	Array of ResourceRes p objects	Vault resources
tags	Array of Tag objects	Vault tags
auto_bind	Boolean	Indicates whether automatic association is enabled. Its default value is false (not enabled).
bind_rules	VaultBindRul es object	Association rule
user_id	String	User ID
created_at	String	Creation time, for example, 2020-02-05T10:38:34.209782
auto_expand	Boolean	Whether to enable auto capacity expansion for the vault.

Table 4-130 Billing

Parameter	Type	Description
allocated	Integer	Allocated capacity, in GB.
charging_mode	String	Billing mode, which is post_paid
cloud_type	String	Cloud type, which is public
consistent_level	String	Vault specification, which is crash_consistent by default (crash consistent backup)
object_type	String	Object type, which can be server , disk , or turbo
order_id	String	Order ID
product_id	String	Product ID
protect_type	String	Protection type, which is backup
size	Integer	Capacity, in GB Minimum: 1 Maximum: 10485760
spec_code	String	Specification code Server backup vault: vault.backup.server.normal ; Disk backup vault: vault.backup.volume.normal ; File system backup vault: vault.backup.turbo.normal
status	String	Vault status Enumeration values: <ul style="list-style-type: none"> • available • lock • frozen • deleting • error
storage_unit	String	Name of the bucket for the vault
used	Integer	Used capacity, in MB.
frozen_scene	String	Scenario when an account is frozen
is_multi_az	Boolean	Multi-AZ attribute of a vault Default: false

Table 4-131 ResourceResp

Parameter	Type	Description
id	String	ID of the resource to be backed up
name	String	Name of the resource to be backed up Minimum: 0 Maximum: 255
protect_status	String	Protection status Enumeration values: <ul style="list-style-type: none"> • available • error • protecting • restoring • removing
size	Integer	Allocated capacity for the associated resources, in GB
type	String	Type of the resource to be backed up, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo
backup_size	Integer	Backup size
backup_count	Integer	Number of backups

Table 4-132 ResourceExtraInfo

Parameter	Type	Description
exclude_volumes	Array of strings	IDs of the disks that will not be backed up. This parameter is used when servers are added to a vault, which include all server disks. But some disks do not need to be backed up. Or in case that a server was previously added and some disks on this server do not need to be backed up.

Table 4-133 Tag

Parameter	Type	Description
key	String	<p>Key</p> <p>It can contain a maximum of 36 characters.</p> <p>It cannot be an empty string.</p> <p>Spaces before and after a key will be discarded.</p> <p>It cannot contain non-printable ASCII characters (0–31) and the following characters: =*<>, /</p> <p>It can contain only letters, digits, hyphens (-), and underscores (_).</p>
value	String	<p>Value</p> <p>It is mandatory when a tag is added and optional when a tag is deleted.</p> <p>It can contain a maximum of 43 characters.</p> <p>It can be an empty string.</p> <p>Spaces before and after a value will be discarded.</p> <p>It cannot contain non-printable ASCII characters (0–31) and the following characters: =*<>, /</p> <p>It can contain only letters, digits, hyphens (-), and underscores (_).</p>

Table 4-134 VaultBindRules

Parameter	Type	Description
tags	Array of BindRulesTags objects	<p>Filters automatically associated resources by tag.</p> <p>Minimum length: 0 characters</p> <p>Maximum length: 5 characters</p> <p>Array Length: 0 - 5</p>

Table 4-135 BindRulesTags

Parameter	Type	Description
key	String	The key cannot contain non-printable ASCII characters (0–31) and the following characters: =*<>, / The key can contain only letters, digits, underscores (_), and hyphens (-).
value	String	The value cannot contain non-printable ASCII characters (0–31) and the following characters: =*<>, / The value can contain only letters, digits, underscores (_), and hyphens (-).

Example Requests

Querying a vault list

```
GET https://{endpoint}/v3/{project_id}/vaults
```

Example Responses

Status code: 200

OK

```
{
  "vaults": [ {
    "id": "a335f9e1-1628-4c64-a7be-38656e5ec19c",
    "name": "vault-8538",
    "description": null,
    "resources": [ ],
    "provider_id": "0daac4c5-6707-4851-97ba-169e36266b66",
    "created_at": "2020-09-04T06:57:37.343535",
    "project_id": "0605767b5780d5762fc5c0118072a564",
    "enterprise_project_id": "0",
    "auto_bind": false,
    "bind_rules": { },
    "auto_expand": false,
    "user_id": "aa2999fa5ae640f28926f8fd79188934",
    "billing": {
      "allocated": 0,
      "cloud_type": "public",
      "consistent_level": "crash_consistent",
      "frozen_scene": null,
      "charging_mode": "post_paid",
      "order_id": null,
      "product_id": null,
      "protect_type": "backup",
      "object_type": "server",
      "spec_code": "vault.backup.server.normal",
      "used": 0,
      "storage_unit": null,
      "status": "available",
      "size": 100
    },
    "tags": [ ]
  } ],
}
```

```
"count" : 50
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.4.4 Modifying a Vault

Function

This API is used to modify a vault based on its ID.

URI

PUT /v3/{project_id}/vaults/{vault_id}

Table 4-136 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
vault_id	Yes	String	Vault ID

Request Parameters

Table 4-137 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Table 4-138 Request body parameters

Parameter	Mandatory	Type	Description
vault	Yes	VaultUpdate object	Request body of modifying a vault

Table 4-139 VaultUpdate

Parameter	Mandatory	Type	Description
billing	No	BillingUpdate object	Bill information
name	No	String	Vault name Minimum: 1 Maximum: 64
auto_bind	No	Boolean	Whether automatic association is supported
bind_rules	No	VaultBindRules object	Association rules
auto_expand	No	Boolean	Whether to enable auto capacity expansion for the vault.
smn_notify	No	Boolean	Exception notification function Default: true
threshold	No	Integer	Vault capacity threshold. If the vault capacity usage exceeds this threshold and smn_notify is true, an exception notification is sent. Minimum: 1 Maximum: 100 Default: 80

Table 4-140 BillingUpdate

Parameter	Mandatory	Type	Description
size	No	Integer	Vault size, in GB Minimum: 1 Maximum: 10485760

Table 4-141 VaultBindRules

Parameter	Mandatory	Type	Description
tags	No	Array of BindRulesTags objects	Filters automatically associated resources by tag. Minimum length: 0 characters Maximum length: 5 characters Array Length: 0 - 5

Table 4-142 BindRulesTags

Parameter	Mandatory	Type	Description
key	Yes	String	The key cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, / The key can contain only letters, digits, underscores (_), and hyphens (-).
value	Yes	String	The value cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, / The value can contain only letters, digits, underscores (_), and hyphens (-).

Response Parameters

Status code: 200

Table 4-143 Response body parameters

Parameter	Type	Description
vault	Vault object	Objects returned after the query by a vault

Table 4-144 Vault

Parameter	Type	Description
billing	Billing object	Operation info

Parameter	Type	Description
description	String	User-defined vault description Minimum: 0 Maximum: 255
id	String	Vault ID
name	String	Vault name Minimum: 1 Maximum: 64
project_id	String	Project ID
provider_id	String	ID of the vault resource type
resources	Array of ResourceRes p objects	Vault resources
tags	Array of Tag objects	Vault tags
auto_bind	Boolean	Indicates whether automatic association is enabled. Its default value is false (not enabled).
bind_rules	VaultBindRul es object	Association rule
user_id	String	User ID
created_at	String	Creation time, for example, 2020-02-05T10:38:34.209782
auto_expand	Boolean	Whether to enable auto capacity expansion for the vault.

Table 4-145 Billing

Parameter	Type	Description
allocated	Integer	Allocated capacity, in GB.
charging_mode	String	Billing mode, which is post_paid
cloud_type	String	Cloud type, which is public
consistent_level	String	Vault specification, which is crash_consistent by default (crash consistent backup)
object_type	String	Object type, which can be server , disk , or turbo

Parameter	Type	Description
order_id	String	Order ID
product_id	String	Product ID
protect_type	String	Protection type, which is backup
size	Integer	Capacity, in GB Minimum: 1 Maximum: 10485760
spec_code	String	Specification code Server backup vault: vault.backup.server.normal ; Disk backup vault: vault.backup.volume.normal ; File system backup vault: vault.backup.turbo.normal
status	String	Vault status Enumeration values: <ul style="list-style-type: none"> • available • lock • frozen • deleting • error
storage_unit	String	Name of the bucket for the vault
used	Integer	Used capacity, in MB.
frozen_scene	String	Scenario when an account is frozen
is_multi_az	Boolean	Multi-AZ attribute of a vault Default: false

Table 4-146 ResourceResp

Parameter	Type	Description
id	String	ID of the resource to be backed up
name	String	Name of the resource to be backed up Minimum: 0 Maximum: 255

Parameter	Type	Description
protect_status	String	Protection status Enumeration values: <ul style="list-style-type: none"> • available • error • protecting • restoring • removing
size	Integer	Allocated capacity for the associated resources, in GB
type	String	Type of the resource to be backed up, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo
backup_size	Integer	Backup size
backup_count	Integer	Number of backups

Table 4-147 ResourceExtraInfo

Parameter	Type	Description
exclude_volumes	Array of strings	IDs of the disks that will not be backed up. This parameter is used when servers are added to a vault, which include all server disks. But some disks do not need to be backed up. Or in case that a server was previously added and some disks on this server do not need to be backed up.

Table 4-148 Tag

Parameter	Type	Description
key	String	Key It can contain a maximum of 36 characters. It cannot be an empty string. Spaces before and after a key will be discarded. It cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, / It can contain only letters, digits, hyphens (-), and underscores (_).

Parameter	Type	Description
value	String	<p>Value</p> <p>It is mandatory when a tag is added and optional when a tag is deleted.</p> <p>It can contain a maximum of 43 characters.</p> <p>It can be an empty string.</p> <p>Spaces before and after a value will be discarded.</p> <p>It cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, /</p> <p>It can contain only letters, digits, hyphens (-), and underscores (_).</p>

Table 4-149 VaultBindRules

Parameter	Type	Description
tags	Array of BindRulesTags objects	<p>Filters automatically associated resources by tag.</p> <p>Minimum length: 0 characters</p> <p>Maximum length: 5 characters</p> <p>Array Length: 0 - 5</p>

Table 4-150 BindRulesTags

Parameter	Type	Description
key	String	<p>The key cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, /</p> <p>The key can contain only letters, digits, underscores (_), and hyphens (-).</p>
value	String	<p>The value cannot contain non-printable ASCII characters (0-31) and the following characters: =*<>, /</p> <p>The value can contain only letters, digits, underscores (_), and hyphens (-).</p>

Example Requests

Modifying a vault (vault capacity changed to 200 GB and vault name changed to **vault_name02**)

```
PUT https://{endpoint}/v3/f841e01fd2b14e7fa41b6ae7aa6b0594/vaults/79bd9daa-884f-4f84-  
b8fe-235d58cd927d  
  
{  
  "vault": {  
    "billing": {  
      "size": 200  
    },  
    "name": "vault_name02"  
  }  
}
```

Example Responses

Status code: 200

OK

```
{  
  "vault": {  
    "name": "vault_name02",  
    "billing": {  
      "status": "available",  
      "used": 0,  
      "protect_type": "backup",  
      "order_id": null,  
      "object_type": "server",  
      "allocated": 40,  
      "spec_code": "vault.backup.server.normal",  
      "size": 200,  
      "cloud_type": "public",  
      "product_id": null,  
      "consistent_level": "crash_consistent",  
      "storage_unit": null,  
      "charging_mode": "post_paid"  
    },  
    "tags": [ {  
      "value": "value01",  
      "key": "key01"  
    } ],  
    "created_at": "2019-05-08T09:31:21.840431",  
    "project_id": "4229d7a45436489f8c3dc2b1d35d4987",  
    "enterprise_project_id": "0",  
    "id": "2402058d-8373-4b0a-b848-d3c0dfdc71a8",  
    "resources": [ {  
      "name": "ecs-1f0f-0003",  
      "protect_status": "available",  
      "extra_info": {  
        "exclude_volumes": [ "bdef09bb-293f-446a-88a4-86e9f14408c4" ]  
      },  
      "type": "OS::Nova::Server",  
      "id": "97595625-198e-4e4d-879b-9d53f68ba551",  
      "size": 40  
    } ],  
    "description": "vault_description"  
  }  
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.4.5 Deleting a Vault

Function

This API is used to delete vaults. Once a vault is deleted, all backups in the vault are cleared.

URI

DELETE /v3/{project_id}/vaults/{vault_id}

Table 4-151 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
vault_id	Yes	String	Vault ID

Request Parameters

Table 4-152 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Response Parameters

None

Example Requests

Deleting a vault

```
DELETE https://{endpoint}/v3/{project_id}/vaults/{vault_id}
```

Example Responses

None

Status Codes

Status Code	Description
204	No Content

Error Codes

See [Error Codes](#).

4.4.6 Dissociating Resources

Function

This API is used to dissociate resources from a vault.

URI

POST /v3/{project_id}/vaults/{vault_id}/removeresources

Table 4-153 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
vault_id	Yes	String	Vault ID

Request Parameters

Table 4-154 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Table 4-155 Request body parameters

Parameter	Mandatory	Type	Description
resource_ids	Yes	Array of strings	IDs of the resources to be removed Minimum length: 1 Maximum length: 256 Array Length: 1 - 256

Response Parameters

Status code: 200

Table 4-156 Response body parameters

Parameter	Type	Description
remove_resource_ids	Array of strings	Removed resource IDs

Example Requests

Dissociating resources from a vault and deleting the backups of the resources

```
POST https://{endpoint}/v3/f841e01fd2b14e7fa41b6ae7aa6b0594/vaults/79bd9daa-884f-4f84-b8fe-235d58cd927d/removeresources
```

```
{
  "resource_ids" : [ "97595625-198e-4e4d-879b-9d53f68ba551" ]
}
```

Example Responses

Status code: 200

OK

```
{
  "remove_resource_ids" : [ "97595625-198e-4e4d-879b-9d53f68ba551" ]
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.4.7 Associating Resources

Function

This API is used to associate resources with a vault.

URI

POST /v3/{project_id}/vaults/{vault_id}/addressesources

Table 4-157 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
vault_id	Yes	String	Vault ID

Request Parameters

Table 4-158 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Table 4-159 Request body parameters

Parameter	Mandatory	Type	Description
resources	Yes	Array of ResourceCreate objects	Resource list Minimum length: 1 Maximum length: 256 Array Length: 1 - 256

Table 4-160 ResourceCreate

Parameter	Mandatory	Type	Description
id	Yes	String	ID of the resource to be backed up

Parameter	Mandatory	Type	Description
type	Yes	String	Type of the resource to be backed up, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo
name	No	String	Resource name Minimum: 0 Maximum: 255

Table 4-161 ResourceExtraInfo

Parameter	Mandatory	Type	Description
exclude_volumes	No	Array of strings	IDs of the disks that will not be backed up. This parameter is used when servers are added to a vault, which include all server disks. But some disks do not need to be backed up. Or in case that a server was previously added and some disks on this server do not need to be backed up.

Response Parameters

Status code: 200

Table 4-162 Response body parameters

Parameter	Type	Description
add_resource_ids	Array of strings	List of resource IDs that have been added

Example Requests

```
POST https://{endpoint}/v3/f841e01fd2b14e7fa41b6ae7aa6b0594/vaults/79bd9daa-884f-4f84-b8fe-235d58cd927d/addresources
```

```
{
  "resources": [ {
    "extra_info": {
      "exclude_volumes": [ "bdef09bb-293f-446a-88a4-86e9f14408c4" ]
    },
    "id": "97595625-198e-4e4d-879b-9d53f68ba551",
    "type": "OS::Nova::Server"
  }
]
```

```
    }]  
  }
```

Example Responses

Status code: 200

OK

```
{  
  "add_resource_ids" : [ "97595625-198e-4e4d-879b-9d53f68ba551" ]  
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.4.8 Applying a Policy to a Vault

Function

This API is used to apply a policy to a vault.

URI

POST /v3/{project_id}/vaults/{vault_id}/associatepolicy

Table 4-163 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
vault_id	Yes	String	Vault ID

Request Parameters

Table 4-164 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Table 4-165 Request body parameters

Parameter	Mandatory	Type	Description
policy_id	No	String	Policy ID.

Response Parameters

Status code: 200

Table 4-166 Response body parameters

Parameter	Type	Description
associate_policy	VaultPolicyResp object	Details of applying a policy to a vault

Table 4-167 VaultPolicyResp

Parameter	Type	Description
policy_id	String	Configured policy ID
vault_id	String	Vault ID for configuring the policy ID

Example Requests

Applying a policy to a vault

```
POST https://{endpoint}/v3/f841e01fd2b14e7fa41b6ae7aa6b0594/vaults/79bd9daa-884f-4f84-b8fe-235d58cd927d/associatepolicy
```

```
{
  "policy_id" : "7075c397-25a0-43e2-a83a-bb16eaca3ee5"
}
```

Example Responses

Status code: 200

OK

```
{
  "associate_policy" : {
    "vault_id" : "2402058d-8373-4b0a-b848-d3c0dfdc71a8",
    "policy_id" : "7075c397-25a0-43e2-a83a-bb16eaca3ee5"
  }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.4.9 Removing a Policy from a Vault

Function

This API is used to remove a policy from a vault.

URI

POST /v3/{project_id}/vaults/{vault_id}/dissociatepolicy

Table 4-168 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
vault_id	Yes	String	Vault ID

Request Parameters

Table 4-169 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Table 4-170 Request body parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID

Response Parameters

Status code: 200

Table 4-171 Response body parameters

Parameter	Type	Description
dissociate_policy	VaultPolicyResp object	Details of removing a policy from a vault

Table 4-172 VaultPolicyResp

Parameter	Type	Description
policy_id	String	Configured policy ID
vault_id	String	Vault ID for configuring the policy ID

Example Requests

Removing a policy from a vault

```
POST https://{endpoint}/v3/f841e01fd2b14e7fa41b6ae7aa6b0594/vaults/79bd9daa-884f-4f84-b8fe-235d58cd927d/dissociatepolicy
```

```
{
  "policy_id" : "7075c397-25a0-43e2-a83a-bb16eaca3ee5"
}
```

Example Responses

Status code: 200

OK

```
{
  "dissociate_policy" : {
    "vault_id" : "2402058d-8373-4b0a-b848-d3c0dfdc71a8",
    "policy_id" : "7075c397-25a0-43e2-a83a-bb16eaca3ee5"
  }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.4.10 Migrating Resources

Function

This API is used to associate resources with another vault and migrate the resource backups to that destination vault.

URI

POST /v3/{project_id}/vaults/{vault_id}/migrateresources

Table 4-173 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID
vault_id	Yes	String	Vault ID

Request Parameters

Table 4-174 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	No	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Table 4-175 Request body parameters

Parameter	Mandatory	Type	Description
destination_vault_id	Yes	String	Destination vault
resource_ids	Yes	Array of strings	ID of the resource to be migrated

Response Parameters

Status code: 200

Table 4-176 Response body parameters

Parameter	Type	Description
migrated_resources	Array of strings	List of migrated resources

Example Requests

Migrating resources as well as their backups to a different vault

```
POST https://{endpoint}/v3/f841e01fd2b14e7fa41b6ae7aa6b0594/vaults/79bd9daa-884f-4f84-b8fe-235d58cd927d/migrateresources
```

```
{
  "resource_ids" : [ "abcdde3f-e0e3-403a-b690-fc259dd70008" ],
  "destination_vault_id" : "fe578a6c-d1a8-4790-bd52-5954af4d446c"
}
```

Example Responses

Status code: 200

OK


```
{
  "migrated_resources" : [ "fe578a6c-d1a8-4790-bd52-5954af4d446c" ]
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.5 Backups

4.5.1 Querying a Specified Backup

Function

This API is used to query the backup of a specific ID.

URI

GET /v3/{project_id}/backups/{backup_id}

Table 4-177 Path Parameters

Parameter	Mandatory	Type	Description
backup_id	Yes	String	Backup ID
project_id	Yes	String	Project ID

Request Parameters

Table 4-178 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Response Parameters

Status code: 200

Table 4-179 Response body parameters

Parameter	Type	Description
backup	BackupResp object	Backup

Table 4-180 BackupResp

Parameter	Type	Description
checkpoint_id	String	Restore point ID
created_at	String	Creation time, for example, 2020-02-05T10:38:34.209782
description	String	Backup description
expired_at	String	Expiration time, for example, 2020-02-05T10:38:34.209782
extend_info	BackupExtendInfo object	Extended information
id	String	Backup ID
image_type	String	Backup type, which is backup .
name	String	Backup name
parent_id	String	Parent backup ID
project_id	String	Project ID
protected_at	String	Backup time
resource_az	String	Resource availability zone
resource_id	String	Resource ID
resource_name	String	Resource name
resource_size	Integer	Resource size, in GB
resource_type	String	Resource type, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo

Parameter	Type	Description
status	String	Backup status Enumeration values: <ul style="list-style-type: none"> • available • protecting • deleting • restoring • error • waiting_protect • waiting_delete • waiting_restore
updated_at	String	Update time, for example, 2020-02-05T10:38:34.209782
vault_id	String	Vault ID
children	Array of BackupResp objects	Backup list

Table 4-181 BackupExtendInfo

Parameter	Type	Description
auto_trigger	Boolean	Whether the backup is automatically generated
bootable	Boolean	Whether the backup is a system disk backup
incremental	Boolean	Whether the backup is an incremental backup
snapshot_id	String	Snapshot ID of the disk backup
support_lld	Boolean	Whether to allow lazyloading for fast restoration

Parameter	Type	Description
supported_restore_mode	String	Restoration mode. Possible values are na , snapshot , and backup . snapshot indicates the backup can be used to create a full-server image. backup indicates the data is restored from backups of the EVS disks of the server. na indicates the backup can only be used to create new resources but cannot be used for restoration. Default: na Enumeration values: <ul style="list-style-type: none"> • na • backup • snapshot
os_images_data	Array of ImageData objects	ID list of images created using backups
contain_system_disk	Boolean	Whether the VM backup data contains system disk data
encrypted	Boolean	Whether the backup is encrypted
system_disk	Boolean	Whether the disk is a system disk
is_multi_az	Boolean	Whether multi-AZ backup redundancy is used Default: false

Table 4-182 ImageData

Parameter	Type	Description
image_id	String	Image ID

Table 4-183 ReplicationRecordsExtraInfo

Parameter	Type	Description
progress	Integer	Replication progress
fail_code	String	Error code. This field is empty if the operation is successful.
fail_reason	String	Error cause
auto_trigger	Boolean	Whether replication is automatically scheduled

Parameter	Type	Description
destination_vault_id	String	Destination vault ID

Example Requests

Querying a backup

```
GET https://{endpoint}/v3/{project_id}/backups/{backup_id}
```

Example Responses

Status code: 200

OK

```
{
  "backup": {
    "provider_id": "0daac4c5-6707-4851-97ba-169e36266b66",
    "checkpoint_id": "8b0851a8-adf3-4f4c-a914-dead08bf9664",
    "enterprise_project_id": "0",
    "updated_at": null,
    "vault_id": "3b5816b5-f29c-4172-9d9a-76c719a659ce",
    "id": "6df2b54c-dd62-4059-a07c-1b8f24f2725d",
    "resource_az": "az1.dc1",
    "image_type": "backup",
    "resource_id": "94eba8b2-acc9-4d82-badc-127144cc5526",
    "resource_size": 40,
    "children": [ {
      "provider_id": "0daac4c5-6707-4851-97ba-169e36266b66",
      "checkpoint_id": "8b0851a8-adf3-4f4c-a914-dead08bf9664",
      "updated_at": null,
      "vault_id": "3b5816b5-f29c-4172-9d9a-76c719a659ce",
      "id": "5d822633-2bbf-4af8-a16e-5ab1c7705235",
      "resource_az": null,
      "image_type": "backup",
      "resource_id": "eccbcfdd-f843-4bbb-b2c0-a5ce861f9376",
      "resource_size": 40,
      "children": [ ],
      "parent_id": "6df2b54c-dd62-4059-a07c-1b8f24f2725d",
      "extend_info": {
        "auto_trigger": true,
        "supported_restore_mode": null,
        "os_images_data": null,
        "snapshot_id": "5230a977-1a94-4092-8edd-519303a44cda",
        "bootable": true,
        "support_llid": null,
        "encrypted": true
      },
      "project_id": "4229d7a45436489f8c3dc2b1d35d4987",
      "status": "available",
      "resource_name": "ecs-1f0f-0002",
      "description": null,
      "expired_at": null,
      "name": "autobk_a843_ecs-1f0f-0002",
      "created_at": "2019-05-10T07:59:59.450700",
      "protected_at": null,
      "resource_type": "OS::Cinder::Volume"
    } ],
    "parent_id": null,
    "extend_info": {
      "auto_trigger": true,
      "supported_restore_mode": "backup",

```

```

"os_images_data" : null,
"contain_system_disk" : true,
"snapshot_id" : null,
"bootable" : null,
"support_llid" : true
},
"project_id" : "4229d7a45436489f8c3dc2b1d35d4987",
"status" : "available",
"resource_name" : "ecs-1f0f-0002",
"description" : "backup_description",
"expired_at" : null,
"name" : "backup_name",
"created_at" : "2019-05-10T07:59:12.084695",
"protected_at" : null,
"resource_type" : "OS::Nova::Server"
}
}

```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.5.2 Querying All Backups

Function

This API is used to query all backups.

URI

GET /v3/{project_id}/backups

Table 4-184 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-185 Query Parameters

Parameter	Mandatory	Type	Description
checkpoint_id	No	String	Restore point ID

Parameter	Mandatory	Type	Description
dec	No	Boolean	Dedicated cloud tag, which only takes effect in dedicated cloud scenarios
end_time	No	String	Time when the backup ends, in %YYYY-%mm-%ddT%HH:%MM:%SSZ format. For example, 2018-02-01T12:00:00Z .
image_type	No	String	Backup type, which is backup .
incremental	No	Boolean	Whether incremental backup is used Default: false
limit	No	Integer	Number of records displayed per page. The value must be a positive integer.
marker	No	String	ID of the last record displayed on the previous page
member_status	No	String	Backup sharing status Enumeration values: <ul style="list-style-type: none"> • pending • accepted • rejected
name	No	String	Backup name
offset	No	Integer	Offset value. The value must be a positive integer.
own_type	No	String	Owning type of a backup. private backups are queried by default. Default: private Enumeration values: <ul style="list-style-type: none"> • all_granted • private • shared
parent_id	No	String	Parent backup ID
resource_az	No	String	AZ-based filtering is supported.
resource_id	No	String	Resource ID

Parameter	Mandatory	Type	Description
resource_name	No	String	Resource name
resource_type	No	String	Resource type, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo
sort	No	String	A group of properties separated by commas (,) and sorting directions. The value is in the format of <key1>[:<direction>],<key2>[:<direction>], where the value of direction is asc (ascending order) or desc (descending order). If a direction is not specified, the default sorting direction is desc . The value of sort can contain a maximum of 255 characters. The key can be as follows: created_at , updated_at , name , status , protected_at , id
start_time	No	String	Time when the backup starts, in %YYYY-%mm-%ddT%HH:%MM:%SSZ format. For example, 2018-02-01T12:00:00Z .
status	No	String	Status When the API is called, multiple statuses can be transferred for filtering, for example, status=available&status=error . Enumeration values: <ul style="list-style-type: none"> ● available ● protecting ● deleting ● restoring ● error ● waiting_protect ● waiting_delete ● waiting_restore

Parameter	Mandatory	Type	Description
used_percent	No	String	Backups are filtered based on the occupied vault capacity. The value ranges from 1 to 100 . For example, if used_percent is set to 80 , all backups who occupied 80% or more of the vault capacity are displayed.
vault_id	No	String	Vault ID

Request Parameters

Table 4-186 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Response Parameters

Status code: 200

Table 4-187 Response body parameters

Parameter	Type	Description
backups	Array of BackupResp objects	Backup list
count	Integer	Number of backups
offset	Integer	Offset where the query starts Minimum: 0 Default: 0
limit	Integer	Number of records displayed on each page Minimum: 1 Maximum: 1000 Default: 1000

Table 4-188 BackupResp

Parameter	Type	Description
checkpoint_id	String	Restore point ID
created_at	String	Creation time, for example, 2020-02-05T10:38:34.209782
description	String	Backup description
expired_at	String	Expiration time, for example, 2020-02-05T10:38:34.209782
extend_info	BackupExtendInfo object	Extended information
id	String	Backup ID
image_type	String	Backup type, which is backup .
name	String	Backup name
parent_id	String	Parent backup ID
project_id	String	Project ID
protected_at	String	Backup time
resource_az	String	Resource availability zone
resource_id	String	Resource ID
resource_name	String	Resource name
resource_size	Integer	Resource size, in GB
resource_type	String	Resource type, which can be OS::Nova::Server , OS::Cinder::Volume , or OS::Sfs::Turbo
status	String	Backup status Enumeration values: <ul style="list-style-type: none"> • available • protecting • deleting • restoring • error • waiting_protect • waiting_delete • waiting_restore
updated_at	String	Update time, for example, 2020-02-05T10:38:34.209782
vault_id	String	Vault ID

Parameter	Type	Description
children	Array of BackupResp objects	Backup list

Table 4-189 BackupExtendInfo

Parameter	Type	Description
auto_trigger	Boolean	Whether the backup is automatically generated
bootable	Boolean	Whether the backup is a system disk backup
incremental	Boolean	Whether the backup is an incremental backup
snapshot_id	String	Snapshot ID of the disk backup
support_llid	Boolean	Whether to allow lazyloading for fast restoration
supported_restoration_mode	String	Restoration mode. Possible values are na , snapshot , and backup . snapshot indicates the backup can be used to create a full-server image. backup indicates the data is restored from backups of the EVS disks of the server. na indicates the backup can only be used to create new resources but cannot be used for restoration. Default: na Enumeration values: <ul style="list-style-type: none"> • na • backup • snapshot
os_images_data	Array of ImageData objects	ID list of images created using backups
contain_system_disk	Boolean	Whether the VM backup data contains system disk data
encrypted	Boolean	Whether the backup is encrypted
system_disk	Boolean	Whether the disk is a system disk
is_multi_az	Boolean	Whether multi-AZ backup redundancy is used Default: false

Table 4-190 ImageData

Parameter	Type	Description
image_id	String	Image ID

Table 4-191 ReplicationRecordsExtraInfo

Parameter	Type	Description
progress	Integer	Replication progress
fail_code	String	Error code. This field is empty if the operation is successful.
fail_reason	String	Error cause
auto_trigger	Boolean	Whether replication is automatically scheduled
destination_vault_id	String	Destination vault ID

Example Requests

Querying all backups

```
GET https://{endpoint}/v3/{project_id}/backups
```

Example Responses

Status code: 200

OK

```
{
  "count" : 2,
  "backups" : [ {
    "provider_id" : "0daac4c5-6707-4851-97ba-169e36266b66",
    "checkpoint_id" : "1fced58b-2a31-4851-bcbb-96216f83ce99",
    "updated_at" : "2020-02-21T07:07:25.113761",
    "vault_id" : "cca85ea5-00a4-418d-9222-bd83985bc515",
    "id" : "b1c4afd9-e7a6-4888-9010-c2bac3aa7910",
    "resource_az" : "br-iaas-odin1a",
    "image_type" : "backup",
    "resource_id" : "1a503932-ee8f-4dd5-8248-8dfb57e584c5",
    "resource_size" : 40,
    "children" : [ ],
    "extend_info" : {
      "auto_trigger" : true,
      "supported_restore_mode" : "backup",
      "contain_system_disk" : true,
      "support_lld" : true,
      "system_disk" : false
    },
    "project_id" : "0605767b5780d5762fc5c0118072a564",
    "status" : "available",
    "resource_name" : "test001-02",
    "description" : "",
    "expired_at" : "2020-05-21T07:00:54.060493",
```

```

"name" : "autobk_b629",
"created_at" : "2020-02-21T07:00:54.065135",
"resource_type" : "OS::Nova::Server"
}, {
  "provider_id" : "d1603440-187d-4516-af25-121250c7cc97",
  "checkpoint_id" : "f64c351f-769f-4c04-8806-fd90a59e9b12",
  "updated_at" : "2020-02-21T07:09:37.767084",
  "vault_id" : "79bd9daa-884f-4f84-b8fe-235d58cd927d",
  "id" : "5606aab5-2dc2-4498-8144-dc848d099af5",
  "resource_az" : "br-iaas-odin1a",
  "image_type" : "backup",
  "resource_id" : "54f7ccbc-072f-4ec5-a7b7-b24dabdb4539",
  "resource_size" : 40,
  "children" : [ ],
  "extend_info" : {
    "auto_trigger" : true,
    "snapshot_id" : "e3def9a8-e4b4-4c12-b132-f4ba8ce9a34f",
    "bootable" : true,
    "support_lld" : true,
    "encrypted" : false,
    "system_disk" : false
  },
  "project_id" : "0605767b5780d5762fc5c0118072a564",
  "status" : "available",
  "resource_name" : "qsy_000",
  "description" : "",
  "expired_at" : "2020-03-22T07:00:34.877896",
  "name" : "autobk_6809",
  "created_at" : "2020-02-21T07:00:34.882174",
  "resource_type" : "OS::Cinder::Volume"
}
}

```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.5.3 Deleting a Backup

Function

This API is used to delete a single backup.

URI

DELETE /v3/{project_id}/backups/{backup_id}

Table 4-192 Path Parameters

Parameter	Mandatory	Type	Description
backup_id	Yes	String	ID of the backup to be deleted
project_id	Yes	String	Project ID

Request Parameters

Table 4-193 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Response Parameters

None

Example Requests

Deleting a backup

```
DELETE https://{endpoint}/v3/{project_id}/backups/{backup_id}
```

Example Responses

None

Status Codes

Status Code	Description
204	No Content

Error Codes

See [Error Codes](#).

4.5.4 Restoring a Backup

Function

This API is used to restore backup data.

URI

POST /v3/{project_id}/backups/{backup_id}/restore

Table 4-194 Path Parameters

Parameter	Mandatory	Type	Description
backup_id	Yes	String	Backup ID
project_id	Yes	String	Project ID

Request Parameters

Table 4-195 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Table 4-196 Request body parameters

Parameter	Mandatory	Type	Description
restore	Yes	BackupRestore object	Request body of restoring a backup

Table 4-197 BackupRestore

Parameter	Mandatory	Type	Description
mappings	No	Array of BackupRestoreServerMapping objects	Restored mapping relationship. This parameter is mandatory for VM restoration and optional for disk restoration.

Parameter	Mandatory	Type	Description
power_on	No	Boolean	Whether the server is powered on after restoration. By default it is powered on after restoration. Default: true
server_id	No	String	ID of the target VM to be restored. This parameter is mandatory for VM restoration.
volume_id	No	String	ID of the target disk to be restored. This parameter is mandatory for disk restoration.

Table 4-198 BackupRestoreServerMapping

Parameter	Mandatory	Type	Description
backup_id	Yes	String	Disk backup ID
volume_id	Yes	String	ID of the disk to which data is restored

Table 4-199 RestoreDetails

Parameter	Mandatory	Type	Description
destination_path	Yes	String	Destination path Minimum: 1 Maximum: 255

Response Parameters

None

Example Requests

Restoring from a specified backup

```
POST https://{endpoint}/v3/{f841e01fd2b14e7fa41b6ae7aa6b0594}/backups/a5200268-74a5-4806-acc6-95793ab0228b/restore
```

```
{
  "restore": {
    "mappings": [ {
      "backup_id": "5d822633-2bbf-4af8-a16e-5ab1c7705235",
      "volume_id": "eccbcfdd-f843-4bbb-b2c0-a5ce861f9376"
    }
  ]
}
```



```
    } ],  
    "power_on" : true,  
    "server_id" : "94eba8b2-acc9-4d82-badc-127144cc5526"  
  }  
}
```

Example Responses

None

Status Codes

Status Code	Description
202	Accepted

Error Codes

See [Error Codes](#).

4.6 Policies

4.6.1 Creating a Policy

Function

This API is used to create a backup policy.

URI

POST /v3/{project_id}/policies

Table 4-200 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Request Parameters

Table 4-201 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Table 4-202 Request body parameters

Parameter	Mandatory	Type	Description
policy	Yes	PolicyCreate object	Request body for creating a policy

Table 4-203 PolicyCreate

Parameter	Mandatory	Type	Description
enabled	No	Boolean	Whether to enable the policy Default: true
name	Yes	String	Specifies the policy name. The value consists of 1 to 64 characters and can contain only letters, digits, underscores (_), and hyphens (-). Minimum: 1 Maximum: 64
operation_definition	Yes	PolicyODCreate object	Scheduling parameter
operation_type	Yes	String	Protection type, which is backup
trigger	Yes	PolicyTriggerReq object	Time rule for the policy execution

Table 4-204 PolicyoODCreate

Parameter	Mandatory	Type	Description
day_backups	No	Integer	Specifies the number of retained daily backups. The latest backup of each day is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100
max_backups	No	Integer	Maximum number of retained backups. The value can be -1 or ranges from 0 to 99999 . If the value is set to -1 , the backups will not be cleared even though the configured retained backup quantity is exceeded. If this parameter and retention_duration_days are both left blank, the backups will be retained permanently. Minimum: 1 Maximum: 99999 Default: -1
month_backups	No	Integer	Specifies the number of retained monthly backups. The latest backup of each month is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100

Parameter	Mandatory	Type	Description
retention_duration_days	No	Integer	Duration of retaining a backup, in days. The maximum value is 99999 . -1 indicates that the backups will not be cleared based on the retention duration. If this parameter and max_backups are left blank at the same time, the backups will be retained permanently. Minimum: 1 Maximum: 99999 Default: -1
timezone	No	String	Time zone where the user is located, for example, UTC +08:00. Set this parameter if you have configured any of the parameters: day_backups , week_backups , month_backups , year_backups .
week_backups	No	Integer	Specifies the number of retained weekly backups. The latest backup of each week is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory.
year_backups	No	Integer	Specifies the number of retained yearly backups. The latest backup of each year is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100

Parameter	Mandatory	Type	Description
full_backup_interval	No	Integer	Defines how often (after how many incremental backups) a full backup is performed. If -1 is specified, full backup will not be performed. Minimum value: -1 Maximum value: 100 Minimum: -1 Maximum: 100

Table 4-205 PolicyTriggerReq

Parameter	Mandatory	Type	Description
properties	Yes	PolicyTriggerPropertiesReq object	Scheduler attributes

Table 4-206 PolicyTriggerPropertiesReq

Parameter	Mandatory	Type	Description
pattern	Yes	Array of strings	Scheduling rule of the scheduler. A maximum of 24 rules can be configured. The scheduling rule complies with iCalendar RFC 2445, but it supports only the FREQ , BYDAY , BYHOUR , BYMINUTE , and INTERVAL parameters. FREQ can be set only to WEEKLY or DAILY . BYDAY can be set to MO , TU , WE , TH , FR , SA , and SU (seven days of a week). BYHOUR ranges from 0 to 23 hours. BYMINUTE ranges from 0 to 59 minutes. The scheduling interval cannot be less than 1 hour. A maximum of 24 time points are allowed in a day. For example, if the scheduling time is 14:00 (UTC) from Monday to Sunday, set the scheduling rule as follows: FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00 . If the scheduling time is 14:00 (UTC +8) every day, set the scheduling rule as follows: FREQ=DAILY;INTERVAL=1;BYHOUR=6;BYMINUTE=00

Response Parameters

Status code: 200

Table 4-207 Response body parameters

Parameter	Type	Description
policy	Policy object	Response to the request for creating a policy

Table 4-208 Policy

Parameter	Type	Description
enabled	Boolean	Whether the policy is enabled
id	String	Policy ID
name	String	Policy Name
operation_definition	PolicyODCreate object	Policy attributes
operation_type	String	Protection type, which is backup Enumeration values: <ul style="list-style-type: none"> • backup • replication
trigger	PolicyTriggerResp object	Time scheduling rule for the policy
associated_vaults	Array of PolicyAssociateVault objects	Associated vault

Table 4-209 PolicyODCreate

Parameter	Type	Description
day_backups	Integer	Specifies the number of retained daily backups. The latest backup of each day is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100

Parameter	Type	Description
max_backups	Integer	<p>Maximum number of retained backups. The value can be -1 or ranges from 0 to 99999. If the value is set to -1, the backups will not be cleared even though the configured retained backup quantity is exceeded. If this parameter and retention_duration_days are both left blank, the backups will be retained permanently.</p> <p>Minimum: 1 Maximum: 99999 Default: -1</p>
month_backups	Integer	<p>Specifies the number of retained monthly backups. The latest backup of each month is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups. The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory.</p> <p>Minimum: 0 Maximum: 100</p>
retention_duration_days	Integer	<p>Duration of retaining a backup, in days. The maximum value is 99999. -1 indicates that the backups will not be cleared based on the retention duration. If this parameter and max_backups are left blank at the same time, the backups will be retained permanently.</p> <p>Minimum: 1 Maximum: 99999 Default: -1</p>
timezone	String	<p>Time zone where the user is located, for example, UTC+08:00. Set this parameter if you have configured any of the parameters: day_backups, week_backups, month_backups, year_backups.</p>
week_backups	Integer	<p>Specifies the number of retained weekly backups. The latest backup of each week is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups. The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory.</p>

Parameter	Type	Description
year_backups	Integer	Specifies the number of retained yearly backups. The latest backup of each year is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100
full_backup_interval	Integer	Defines how often (after how many incremental backups) a full backup is performed. If -1 is specified, full backup will not be performed. Minimum value: -1 Maximum value: 100 Minimum: -1 Maximum: 100

Table 4-210 PolicyTriggerResp

Parameter	Type	Description
id	String	Scheduler ID
name	String	Scheduler name
properties	PolicyTriggerPropertiesResp object	Scheduler attributes
type	String	Scheduler type. Currently, only time (periodic scheduling) is supported. Enumeration values: <ul style="list-style-type: none"> time

Table 4-211 PolicyTriggerPropertiesResp

Parameter	Type	Description
pattern	Array of strings	Scheduling rule of the scheduler. A maximum of 24 rules can be configured. The scheduling rule complies with iCalendar RFC 2445, but it supports only the FREQ , BYDAY , BYHOUR , BYMINUTE , and INTERVAL parameters. FREQ can be set only to WEEKLY or DAILY . BYDAY can be set to MO , TU , WE , TH , FR , SA , and SU (seven days of a week). BYHOUR ranges from 0 to 23 hours. BYMINUTE ranges from 0 to 59 minutes. The scheduling interval cannot be less than 1 hour. A maximum of 24 time points are allowed in a day. For example, if the scheduling time is 14:00 (UTC) from Monday to Sunday, set the scheduling rule as follows: FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00 . If the scheduling time is 14:00 (UTC+8) every day, set the scheduling rule as follows: FREQ=DAILY;INTERVAL=1;BYHOUR=6;BYMINUTE=00
start_time	String	Start time of the scheduler, for example, 2020-01-08 09:59:49

Table 4-212 PolicyAssociateVault

Parameter	Type	Description
destination_vault_id	String	ID of the associated remote vault
vault_id	String	Vault ID

Example Requests

Creating a backup policy with backups automatically executed at 14:00 everyday and with each backup saved for one day

POST https://{endpoint}/v3/f841e01fd2b14e7fa41b6ae7aa6b0594/policies

```
{
  "policy" : {
    "enabled" : true,
    "name" : "policy001",
    "operation_definition" : {
      "day_backups" : 0,
      "month_backups" : 0,
      "retention_duration_days" : 1,
      "timezone" : "UTC+08:00",
      "week_backups" : 0,

```

```
"year_backups" : 0
},
"operation_type" : "backup",
"trigger" : {
  "properties" : {
    "pattern" : [ "FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00" ]
  }
}
}
```

Example Responses

Status code: 200

OK

```
{
  "policy" : {
    "name" : "policy001",
    "associated_vaults" : null,
    "enabled" : true,
    "trigger" : {
      "properties" : {
        "pattern" : [ "FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00" ],
        "start_time" : "2019-05-08 06:57:05"
      },
      "type" : "time",
      "id" : "d67269a6-5369-42d7-8150-5254bd446328",
      "name" : "default"
    },
    "operation_definition" : {
      "retention_duration_days" : 1,
      "year_backups" : 0,
      "day_backups" : 0,
      "month_backups" : 0,
      "week_backups" : 0,
      "timezone" : "UTC+08:00"
    },
    "operation_type" : "backup",
    "id" : "cbb3ce6f-3332-4e7c-b98e-77290d8471ff"
  }
}
```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.6.2 Querying a Single Policy

Function

This API is used to query a single policy.

URI

GET /v3/{project_id}/policies/{policy_id}

Table 4-213 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID
project_id	Yes	String	Project ID

Request Parameters

Table 4-214 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token. Default: MIIDkgYJKoZIhvc-NAQcCoIIDgzCCXXXXX...

Response Parameters

Status code: 200

Table 4-215 Response body parameters

Parameter	Type	Description
policy	Policy object	Response to the request for creating a policy

Table 4-216 Policy

Parameter	Type	Description
enabled	Boolean	Whether the policy is enabled
id	String	Policy ID
name	String	Policy Name

Parameter	Type	Description
operation_definition	PolicyODCreate object	Policy attributes
operation_type	String	Protection type, which is backup Enumeration values: <ul style="list-style-type: none"> • backup • replication
trigger	PolicyTriggerResp object	Time scheduling rule for the policy
associated_vaults	Array of PolicyAssociateVault objects	Associated vault

Table 4-217 PolicyODCreate

Parameter	Type	Description
day_backups	Integer	Specifies the number of retained daily backups. The latest backup of each day is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100
max_backups	Integer	Maximum number of retained backups. The value can be -1 or ranges from 0 to 99999 . If the value is set to -1 , the backups will not be cleared even though the configured retained backup quantity is exceeded. If this parameter and retention_duration_days are both left blank, the backups will be retained permanently. Minimum: 1 Maximum: 99999 Default: -1

Parameter	Type	Description
month_backups	Integer	Specifies the number of retained monthly backups. The latest backup of each month is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100
retention_duration_days	Integer	Duration of retaining a backup, in days. The maximum value is 99999 . -1 indicates that the backups will not be cleared based on the retention duration. If this parameter and max_backups are left blank at the same time, the backups will be retained permanently. Minimum: 1 Maximum: 99999 Default: -1
timezone	String	Time zone where the user is located, for example, UTC+08:00. Set this parameter if you have configured any of the parameters: day_backups , week_backups , month_backups , year_backups .
week_backups	Integer	Specifies the number of retained weekly backups. The latest backup of each week is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory.
year_backups	Integer	Specifies the number of retained yearly backups. The latest backup of each year is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100

Parameter	Type	Description
full_backup_interval	Integer	Defines how often (after how many incremental backups) a full backup is performed. If -1 is specified, full backup will not be performed. Minimum value: -1 Maximum value: 100 Minimum: -1 Maximum: 100

Table 4-218 PolicyTriggerResp

Parameter	Type	Description
id	String	Scheduler ID
name	String	Scheduler name
properties	PolicyTriggerPropertiesResp object	Scheduler attributes
type	String	Scheduler type. Currently, only time (periodic scheduling) is supported. Enumeration values: <ul style="list-style-type: none"> time

Table 4-219 PolicyTriggerPropertiesResp

Parameter	Type	Description
pattern	Array of strings	Scheduling rule of the scheduler. A maximum of 24 rules can be configured. The scheduling rule complies with iCalendar RFC 2445, but it supports only the FREQ , BYDAY , BYHOUR , BYMINUTE , and INTERVAL parameters. FREQ can be set only to WEEKLY or DAILY . BYDAY can be set to MO , TU , WE , TH , FR , SA , and SU (seven days of a week). BYHOUR ranges from 0 to 23 hours. BYMINUTE ranges from 0 to 59 minutes. The scheduling interval cannot be less than 1 hour. A maximum of 24 time points are allowed in a day. For example, if the scheduling time is 14:00 (UTC) from Monday to Sunday, set the scheduling rule as follows: FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00 . If the scheduling time is 14:00 (UTC+8) every day, set the scheduling rule as follows: FREQ=DAILY;INTERVAL=1;BYHOUR=6;BYMINUTE=00
start_time	String	Start time of the scheduler, for example, 2020-01-08 09:59:49

Table 4-220 PolicyAssociateVault

Parameter	Type	Description
destination_vault_id	String	ID of the associated remote vault
vault_id	String	Vault ID

Example Requests

Querying a policy

```
GET https://{endpoint}/v3/{project_id}/policies/{policy_id}
```

Example Responses

Status code: 200

OK

```
{
  "policy": {
    "name": "policy001",
    "associated_vaults": [ ],
```



```

"enabled" : true,
"trigger" : {
  "properties" : {
    "pattern" : [ "FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00" ],
    "start_time" : "2019-05-08 06:57:05"
  },
  "type" : "time",
  "id" : "d67269a6-5369-42d7-8150-5254bd446328",
  "name" : "default"
},
"operation_definition" : {
  "retention_duration_days" : 1,
  "year_backups" : 0,
  "day_backups" : 0,
  "month_backups" : 0,
  "week_backups" : 0,
  "timezone" : "UTC+08:00"
},
"operation_type" : "backup",
"id" : "cbb3ce6f-3332-4e7c-b98e-77290d8471ff"
}

```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.6.3 Querying the Policy List

Function

This API is used to query the policy list.

URI

GET /v3/{project_id}/policies

Table 4-221 Path Parameters

Parameter	Mandatory	Type	Description
project_id	Yes	String	Project ID

Table 4-222 Query Parameters

Parameter	Mandatory	Type	Description
operation_type	No	String	Policy type Enumeration values: <ul style="list-style-type: none"> • backup • replication
vault_id	No	String	Vault ID

Request Parameters

Table 4-223 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Response Parameters

Status code: 200

Table 4-224 Response body parameters

Parameter	Type	Description
policies	Array of Policy objects	Policy list
count	Integer	Total number of policies

Table 4-225 Policy

Parameter	Type	Description
enabled	Boolean	Whether the policy is enabled
id	String	Policy ID
name	String	Policy Name

Parameter	Type	Description
operation_definition	PolicyODCreate object	Policy attributes
operation_type	String	Protection type, which is backup Enumeration values: <ul style="list-style-type: none"> • backup • replication
trigger	PolicyTriggerResp object	Time scheduling rule for the policy
associated_vaults	Array of PolicyAssociateVault objects	Associated vault

Table 4-226 PolicyODCreate

Parameter	Type	Description
day_backups	Integer	Specifies the number of retained daily backups. The latest backup of each day is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100
max_backups	Integer	Maximum number of retained backups. The value can be -1 or ranges from 0 to 99999 . If the value is set to -1 , the backups will not be cleared even though the configured retained backup quantity is exceeded. If this parameter and retention_duration_days are both left blank, the backups will be retained permanently. Minimum: 1 Maximum: 99999 Default: -1

Parameter	Type	Description
month_backups	Integer	Specifies the number of retained monthly backups. The latest backup of each month is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100
retention_duration_days	Integer	Duration of retaining a backup, in days. The maximum value is 99999 . -1 indicates that the backups will not be cleared based on the retention duration. If this parameter and max_backups are left blank at the same time, the backups will be retained permanently. Minimum: 1 Maximum: 99999 Default: -1
timezone	String	Time zone where the user is located, for example, UTC+08:00. Set this parameter if you have configured any of the parameters: day_backups , week_backups , month_backups , year_backups .
week_backups	Integer	Specifies the number of retained weekly backups. The latest backup of each week is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory.
year_backups	Integer	Specifies the number of retained yearly backups. The latest backup of each year is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100

Parameter	Type	Description
full_backup_interval	Integer	Defines how often (after how many incremental backups) a full backup is performed. If -1 is specified, full backup will not be performed. Minimum value: -1 Maximum value: 100 Minimum: -1 Maximum: 100

Table 4-227 PolicyTriggerResp

Parameter	Type	Description
id	String	Scheduler ID
name	String	Scheduler name
properties	PolicyTriggerPropertiesResp object	Scheduler attributes
type	String	Scheduler type. Currently, only time (periodic scheduling) is supported. Enumeration values: <ul style="list-style-type: none"> time

Table 4-228 PolicyTriggerPropertiesResp

Parameter	Type	Description
pattern	Array of strings	Scheduling rule of the scheduler. A maximum of 24 rules can be configured. The scheduling rule complies with iCalendar RFC 2445, but it supports only the FREQ , BYDAY , BYHOUR , BYMINUTE , and INTERVAL parameters. FREQ can be set only to WEEKLY or DAILY . BYDAY can be set to MO , TU , WE , TH , FR , SA , and SU (seven days of a week). BYHOUR ranges from 0 to 23 hours. BYMINUTE ranges from 0 to 59 minutes. The scheduling interval cannot be less than 1 hour. A maximum of 24 time points are allowed in a day. For example, if the scheduling time is 14:00 (UTC) from Monday to Sunday, set the scheduling rule as follows: FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00 . If the scheduling time is 14:00 (UTC+8) every day, set the scheduling rule as follows: FREQ=DAILY;INTERVAL=1;BYHOUR=6;BYMINUTE=00
start_time	String	Start time of the scheduler, for example, 2020-01-08 09:59:49

Table 4-229 PolicyAssociateVault

Parameter	Type	Description
destination_vault_id	String	ID of the associated remote vault
vault_id	String	Vault ID

Example Requests

Querying the backup policy list

```
GET https://{endpoint}/v3/{project_id}/policies
```

Example Responses

Status code: 200

OK

```
{
  "policies" : [ {
    "name" : "policy001",
    "associated_vaults" : [ ],
```

```

"enabled" : true,
"trigger" : {
  "properties" : {
    "pattern" : [ "FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00" ],
    "start_time" : "2019-05-08 06:57:05"
  },
  "type" : "time",
  "id" : "d67269a6-5369-42d7-8150-5254bd446328",
  "name" : "default"
},
"operation_definition" : {
  "retention_duration_days" : 1,
  "year_backups" : 0,
  "day_backups" : 0,
  "month_backups" : 0,
  "week_backups" : 0,
  "timezone" : "UTC+08:00"
},
"operation_type" : "backup",
"id" : "cbb3ce6f-3332-4e7c-b98e-77290d8471ff"
}],
"count" : 10
}

```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.6.4 Modifying a Policy

Function

This API is used to modify a policy.

URI

PUT /v3/{project_id}/policies/{policy_id}

Table 4-230 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID
project_id	Yes	String	Project ID

Request Parameters

Table 4-231 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Table 4-232 Request body parameters

Parameter	Mandatory	Type	Description
policy	Yes	PolicyUpdate object	Request body of modifying a policy

Table 4-233 PolicyUpdate

Parameter	Mandatory	Type	Description
enabled	No	Boolean	Whether to enable the policy Default: true
name	No	String	Policy Name Minimum: 1 Maximum: 64
operation_definition	No	PolicyODCreate object	Scheduling parameter
trigger	No	PolicyTriggerReq object	Time rule for the policy execution

Table 4-234 PolicyoODCreate

Parameter	Mandatory	Type	Description
day_backups	No	Integer	Specifies the number of retained daily backups. The latest backup of each day is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100
max_backups	No	Integer	Maximum number of retained backups. The value can be -1 or ranges from 0 to 99999 . If the value is set to -1 , the backups will not be cleared even though the configured retained backup quantity is exceeded. If this parameter and retention_duration_days are both left blank, the backups will be retained permanently. Minimum: 1 Maximum: 99999 Default: -1
month_backups	No	Integer	Specifies the number of retained monthly backups. The latest backup of each month is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100

Parameter	Mandatory	Type	Description
retention_duration_days	No	Integer	Duration of retaining a backup, in days. The maximum value is 99999 . -1 indicates that the backups will not be cleared based on the retention duration. If this parameter and max_backups are left blank at the same time, the backups will be retained permanently. Minimum: 1 Maximum: 99999 Default: -1
timezone	No	String	Time zone where the user is located, for example, UTC +08:00. Set this parameter if you have configured any of the parameters: day_backups , week_backups , month_backups , year_backups .
week_backups	No	Integer	Specifies the number of retained weekly backups. The latest backup of each week is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory.
year_backups	No	Integer	Specifies the number of retained yearly backups. The latest backup of each year is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100

Parameter	Mandatory	Type	Description
full_backup_interval	No	Integer	Defines how often (after how many incremental backups) a full backup is performed. If -1 is specified, full backup will not be performed. Minimum value: -1 Maximum value: 100 Minimum: -1 Maximum: 100

Table 4-235 PolicyTriggerReq

Parameter	Mandatory	Type	Description
properties	Yes	PolicyTriggerPropertiesReq object	Scheduler attributes

Table 4-236 PolicyTriggerPropertiesReq

Parameter	Mandatory	Type	Description
pattern	Yes	Array of strings	Scheduling rule of the scheduler. A maximum of 24 rules can be configured. The scheduling rule complies with iCalendar RFC 2445, but it supports only the FREQ , BYDAY , BYHOUR , BYMINUTE , and INTERVAL parameters. FREQ can be set only to WEEKLY or DAILY . BYDAY can be set to MO , TU , WE , TH , FR , SA , and SU (seven days of a week). BYHOUR ranges from 0 to 23 hours. BYMINUTE ranges from 0 to 59 minutes. The scheduling interval cannot be less than 1 hour. A maximum of 24 time points are allowed in a day. For example, if the scheduling time is 14:00 (UTC) from Monday to Sunday, set the scheduling rule as follows: FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00 . If the scheduling time is 14:00 (UTC +8) every day, set the scheduling rule as follows: FREQ=DAILY;INTERVAL=1;BYHOUR=6;BYMINUTE=00

Response Parameters

Status code: 200

Table 4-237 Response body parameters

Parameter	Type	Description
policy	Policy object	Response to the request for creating a policy

Table 4-238 Policy

Parameter	Type	Description
enabled	Boolean	Whether the policy is enabled
id	String	Policy ID
name	String	Policy Name
operation_definition	PolicyODCreate object	Policy attributes
operation_type	String	Protection type, which is backup Enumeration values: <ul style="list-style-type: none"> • backup • replication
trigger	PolicyTriggerResp object	Time scheduling rule for the policy
associated_vaults	Array of PolicyAssociateVault objects	Associated vault

Table 4-239 PolicyODCreate

Parameter	Type	Description
day_backups	Integer	Specifies the number of retained daily backups. The latest backup of each day is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100

Parameter	Type	Description
max_backups	Integer	<p>Maximum number of retained backups. The value can be -1 or ranges from 0 to 99999. If the value is set to -1, the backups will not be cleared even though the configured retained backup quantity is exceeded. If this parameter and retention_duration_days are both left blank, the backups will be retained permanently.</p> <p>Minimum: 1 Maximum: 99999 Default: -1</p>
month_backups	Integer	<p>Specifies the number of retained monthly backups. The latest backup of each month is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups. The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory.</p> <p>Minimum: 0 Maximum: 100</p>
retention_duration_days	Integer	<p>Duration of retaining a backup, in days. The maximum value is 99999. -1 indicates that the backups will not be cleared based on the retention duration. If this parameter and max_backups are left blank at the same time, the backups will be retained permanently.</p> <p>Minimum: 1 Maximum: 99999 Default: -1</p>
timezone	String	<p>Time zone where the user is located, for example, UTC+08:00. Set this parameter if you have configured any of the parameters: day_backups, week_backups, month_backups, year_backups.</p>
week_backups	Integer	<p>Specifies the number of retained weekly backups. The latest backup of each week is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups. The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory.</p>

Parameter	Type	Description
year_backups	Integer	Specifies the number of retained yearly backups. The latest backup of each year is saved in the long term. This parameter can be effective together with the maximum number of retained backups specified by max_backups . The value ranges from 0 to 100. If this parameter is configured, timezone is mandatory. Minimum: 0 Maximum: 100
full_backup_interval	Integer	Defines how often (after how many incremental backups) a full backup is performed. If -1 is specified, full backup will not be performed. Minimum value: -1 Maximum value: 100 Minimum: -1 Maximum: 100

Table 4-240 PolicyTriggerResp

Parameter	Type	Description
id	String	Scheduler ID
name	String	Scheduler name
properties	PolicyTriggerPropertiesResp object	Scheduler attributes
type	String	Scheduler type. Currently, only time (periodic scheduling) is supported. Enumeration values: <ul style="list-style-type: none"> • time

Table 4-241 PolicyTriggerPropertiesResp

Parameter	Type	Description
pattern	Array of strings	Scheduling rule of the scheduler. A maximum of 24 rules can be configured. The scheduling rule complies with iCalendar RFC 2445, but it supports only the FREQ , BYDAY , BYHOUR , BYMINUTE , and INTERVAL parameters. FREQ can be set only to WEEKLY or DAILY . BYDAY can be set to MO , TU , WE , TH , FR , SA , and SU (seven days of a week). BYHOUR ranges from 0 to 23 hours. BYMINUTE ranges from 0 to 59 minutes. The scheduling interval cannot be less than 1 hour. A maximum of 24 time points are allowed in a day. For example, if the scheduling time is 14:00 (UTC) from Monday to Sunday, set the scheduling rule as follows: FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00 . If the scheduling time is 14:00 (UTC+8) every day, set the scheduling rule as follows: FREQ=DAILY;INTERVAL=1;BYHOUR=6;BYMINUTE=00
start_time	String	Start time of the scheduler, for example, 2020-01-08 09:59:49

Table 4-242 PolicyAssociateVault

Parameter	Type	Description
destination_vault_id	String	ID of the associated remote vault
vault_id	String	Vault ID

Example Requests

Modifying a backup policy with backups automatically executed at 14:00 everyday and with each backup saved for one day

```
PUT https://{endpoint}/v3/f841e01fd2b14e7fa41b6ae7aa6b0594/policies/cbb3ce6f-3332-4e7c-b98e-77290d8471ff
```

```
{
  "policy": {
    "enabled": true,
    "name": "policy001",
    "operation_definition": {
      "day_backups": 0,
      "month_backups": 0,
      "max_backups": 1,
      "timezone": "UTC+08:00",
```



```

    "week_backups" : 0,
    "year_backups" : 0
  },
  "trigger" : {
    "properties" : {
      "pattern" : [ "FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00" ]
    }
  }
}
}
}

```

Example Responses

Status code: 200

OK

```

{
  "policy" : {
    "name" : "policy001",
    "associated_vaults" : [ ],
    "enabled" : true,
    "trigger" : {
      "properties" : {
        "pattern" : [ "FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR,SA,SU;BYHOUR=14;BYMINUTE=00" ],
        "start_time" : "2019-05-08 06:57:05"
      },
      "type" : "time",
      "id" : "d67269a6-5369-42d7-8150-5254bd446328",
      "name" : "default"
    },
    "operation_definition" : {
      "max_backups" : 1,
      "year_backups" : 0,
      "day_backups" : 0,
      "month_backups" : 0,
      "week_backups" : 0,
      "timezone" : "UTC+08:00"
    },
    "operation_type" : "backup",
    "id" : "cbb3ce6f-3332-4e7c-b98e-77290d8471ff"
  }
}

```

Status Codes

Status Code	Description
200	OK

Error Codes

See [Error Codes](#).

4.6.5 Deleting a Policy

Function

This API is used to delete a policy.

URI

DELETE /v3/{project_id}/policies/{policy_id}

Table 4-243 Path Parameters

Parameter	Mandatory	Type	Description
policy_id	Yes	String	Policy ID
project_id	Yes	String	Project ID

Request Parameters

Table 4-244 Request header parameters

Parameter	Mandatory	Type	Description
X-Auth-Token	Yes	String	User token The token can be obtained by calling the IAM API used to obtain a user token. The value of X-Subject-Token in the response header is the user token.

Response Parameters

None

Example Requests

Deleting a backup policy

```
DELETE https://{endpoint}/v3/{project_id}/policies/{policy_id}
```

Example Responses

None

Status Codes

Status Code	Description
204	No Content

Error Codes

See [Error Codes](#).

5 Application Cases

[5.1 Example 1: Creating an ECS Backup](#)

[5.2 Example 2: Implementing Automatic Backup for a Vault](#)

[5.3 Example 3: Querying Backups](#)

5.1 Example 1: Creating an ECS Backup

Scenarios

You can back up resources including cloud servers and disks. This section uses an ECS as an example to describe how to create a cloud server backup by calling APIs. For details on how to call APIs, see [3 Calling APIs](#).

Involved APIs

To create a cloud server backup, you need to create a vault for storing backups, associate the target server with the vault, and then back up the server. The following APIs are required:

- [Creating a Vault](#): Create a container for storing backups.
- [Associating Resources](#): Determine the cloud server or disk to be backed up.
- [Creating a Restore Point](#): Create a backup.
- [Querying a Restore Point](#): Confirm that a backup has been created.

Procedure

1. Create a vault.
 - a. Create a vault with simple configurations.
 - API
URI format: POST /v3/{project_id}/vaults
For details, see [Creating a Vault](#).
 - Sample request

POST: `https://{endpoint}/v3/{project_id}/vaults`

Obtain the value of **{endpoint}** from [Regions and Endpoints](#).

Body:

```
{
  "vault": {
    "billing": {
      "cloud_type": "public",
      "consistent_level": "crash_consistent",
      "object_type": "server",
      "protect_type": "backup",
      "size": 200
    },
    "name": "my_vault",
    "resources": []
  }
}
```

- Sample response

```
{
  "vault": {
    "id": "ea7b8717-2543-478a-a92d-3ca7ee448f67",
    "name": "my_vault",
    "description": null,
    "resources": [],
    "provider_id": "0daac4c5-6707-4851-97ba-169e36266b66",
    "created_at": "2020-08-17T03:51:24.678916",
    "project_id": "0605767b5780d5762fc5c0118072a564",
    "enterprise_project_id": "0",
    "auto_bind": false,
    "bind_rules": {},
    "user_id": "aa2999fa5ae640f28926f8fd79188934",
    "billing": {
      "allocated": 0,
      "cloud_type": "public",
      "consistent_level": "crash_consistent",
      "frozen_scene": null,
      "charging_mode": "post_paid",
      "order_id": null,
      "product_id": null,
      "protect_type": "backup",
      "object_type": "server",
      "spec_code": "vault.backup.server.normal",
      "used": 0,
      "storage_unit": null,
      "status": "available",
      "size": 200
    },
    "tags": []
  }
}
```

2. Associate a server or disk with the vault.

- a. Associate resources.

- API

URI format: `POST /v3/{project_id}/vaults/{vault_id}/addressources`

For details, see [Associating Resources](#).

- Sample request

POST: `https://{endpoint}/v3/0605767b5780d5762fc5c0118072a564 / vaults/ea7b8717-2543-478a-a92d-3ca7ee448f67/addressources`

Obtain the value of **{endpoint}** from [Regions and Endpoints](#).

Body:

```
{
  "resources": [{
    "id": "e8cc6bfd-d324-4b88-9109-9fb0ba70676f",
    "type": "OS::Nova::Server",
    "name": "server-4690-0002"
  }]
}
```

- Sample response

```
{
  "add_resource_ids": [
    "e8cc6bfd-d324-4b88-9109-9fb0ba70676f"
  ]
}
```

- b. In the request body, select the ID of an ECS that is in the **Running** state and has not been associated with a vault.

3. Create a restore point.

- a. Create a restore point.

- API

URI format: POST /v3/{project_id}/checkpoints

For details, see [Creating a Restore Point](#).

- Sample request

POST: https://{endpoint}/v3/0605767b5780d5762fc5c0118072a564/checkpoints

Obtain the value of **{endpoint}** from [Regions and Endpoints](#).

Body:

```
{
  "checkpoint": {
    "parameters": {
      "auto_trigger": false,
      "description": "backupauto",
      "incremental": true,
      "name": "backup_auto",
      "resources": ["e8cc6bfd-d324-4b88-9109-9fb0ba70676f"]
    },
    "vault_id": "ea7b8717-2543-478a-a92d-3ca7ee448f67"
  }
}
```

- Sample response

```
{
  "checkpoint": {
    "id": "d9ce6924-d753-4132-bd16-a9f8838ea7d2",
    "project_id": "0605767b5780d5762fc5c0118072a564",
    "status": "protecting",
    "vault": {
      "id": "ea7b8717-2543-478a-a92d-3ca7ee448f67",
      "name": "my_vault",
      "resources": [
        {
          "id": "e8cc6bfd-d324-4b88-9109-9fb0ba70676f",
          "type": "OS::Nova::Server",
          "name": "ecs-9f93-0002",
          "extra_info": "{}",
          "resource_size": "40",
          "backup_size": "0",
          "backup_count": "0",
          "protect_status": "available"
        }
      ]
    }
  },
}
```

```

    "skipped_resources": []
  },
  "created_at": "2020-08-17T06:49:06.307378",
  "extra_info": {
    "name": "backup_auto",
    "description": "backupauto",
    "retention_duration": -1
  }
}

```

- b. Record the ID of the restore point in the response message body.
4. Verify that the server is backed up successfully.
 - API

URI format: GET /v3/{project_id}/checkpoints/{checkpoint_id}

For details, see [Querying a Restore Point](#).

Obtain the value of **{endpoint}** from [Regions and Endpoints](#).

- Sample request

GET: https://{endpoint}/v3/0605767b5780d5762fc5c0118072a564/checkpoints/d9ce6924-d753-4132-bd16-a9f8838ea7d2

- Sample response

```

{
  "checkpoint": {
    "id": "d9ce6924-d753-4132-bd16-a9f8838ea7d2",
    "project_id": "0605767b5780d5762fc5c0118072a564",
    "status": "available",
    "vault": null,
    "created_at": "2020-08-17T06:49:06.260790",
    "extra_info": null
  }
}

```

5.2 Example 2: Implementing Automatic Backup for a Vault

Scenarios

This section describes how to use APIs to set a backup policy and apply the policy to a vault for automatic backup.

Involved APIs

- [Creating a Policy](#): Define when a backup task runs and how long the backups are retained.
- [Applying a Policy to a Vault](#): Apply a policy to a vault.

Procedure

1. Create a backup policy.
 - API

URI format: POST /v3/{project_id}/policies

For details, see [Creating a Policy](#).

- Sample request

POST: <https://{endpoint}/v3/0605767b5780d5762fc5c0118072a564/policies>

Obtain the value of **{endpoint}** from [Regions and Endpoints](#).

Body:

```
{
  "policy": {
    "name": "dh_test_policy",
    "trigger": {
      "properties": {
        "pattern":
["FREQ=WEEKLY;BYDAY=SU,MO,TU,WE,TH,FR,SA;BYHOUR=23;BYMINUTE=00"]
      }
    },
    "operation_definition": {
      "retention_duration_days": 30
    }
  }
}
```

- Sample response

```
{
  "policy": {
    "id": "30d7cf2d-14fc-415b-b7da-858b37f47250",
    "name": "dh_test_policy",
    "operation_type": "backup",
    "operation_definition": {
      "retention_duration_days": 30
    },
    "enabled": true,
    "trigger": {
      "id": "7954175b-ef2c-432c-b936-f6c83df7a593",
      "name": "default",
      "type": "time",
      "properties": {
        "pattern": [
          "FREQ=WEEKLY;BYDAY=SU,MO,TU,WE,TH,FR,SA;BYHOUR=23;BYMINUTE=00"
        ],
        "start_time": "2020-08-17 08:39:44"
      }
    },
    "associated_vaults": null
  }
}
```

2. Apply the policy to a vault.

- API

POST [/v3/{project_id}/vaults/{vault_id}/associatepolicy](https://{endpoint}/v3/{project_id}/vaults/{vault_id}/associatepolicy)

For details, see [Applying a Policy to a Vault](#).

- Sample request

POST: [https://{endpoint}/v3/0605767b5780d5762fc5c0118072a564 / vaults/ea7b8717-2543-478a-a92d-3ca7ee448f67/associatepolicy](https://{endpoint}/v3/0605767b5780d5762fc5c0118072a564/vaults/ea7b8717-2543-478a-a92d-3ca7ee448f67/associatepolicy)

Obtain the value of **{endpoint}** from [Regions and Endpoints](#).

Body:

```
{
  "policy_id": "30d7cf2d-14fc-415b-b7da-858b37f47250"
}
```

- Sample response

```
{
  "associate_policy": {
    "vault_id": "ea7b8717-2543-478a-a92d-3ca7ee448f67",
  }
}
```



```

    "policy_id": "30d7cf2d-14fc-415b-b7da-858b37f47250"
  }
}

```

5.3 Example 3: Querying Backups

Scenarios

This section describes how to use APIs to query all backups of a tenant by page.

The operations described in this section include information query by page and data filtering and sorting. For details about the parameters, see [Querying All Backups](#).

Involved APIs

Querying backups involves the following APIs:

- [Querying backups based on a given limit and offset](#)
- [Querying backups based on a given resource type](#)

Procedure

1. Query backups based on a given **limit** and **offset**.

– API

URI format: GET /v3/{project_id}/backups

For details, see [Querying All Backups](#).

– Sample request

GET:https://{endpoint}/v3/0605767b5780d5762fc5c0118072a564/backups?limit=100&offset=0

Obtain the value of **{endpoint}** from [Regions and Endpoints](#).

– Sample response

```

{
  "backups": [
    .....
    {
      "children": [],
      "checkpoint_id": "e6aec7a9-7b03-4c1d-8a07-5983b53c53f3",
      "created_at": "2020-08-18T06:00:45.375070",
      "description": null,
      "expired_at": null,
      "extend_info": {
        },
      "auto_trigger": true,
      "bootable": null,
      "os_images_data": null,
      "progress": null,
      "snapshot_id": null,
      "support_ll": false,
      "supported_restore_mode": "backup",
      "system_disk": false,
      "contain_system_disk": true,
      "architecture": "x86_64"
    },
    "id": "62617971-839d-4d23-8dfd-4ca65c039bdf",
    "image_type": "backup",
    "name": "autobk_cf91_0003",

```

```

    "parent_id": null,
    "project_id": "0605767b5780d5762fc5c0118072a564",
    "protected_at": "2020-08-18T06:01:10.432117",
    "provider_id": "0daac4c5-6707-4851-97ba-169e36266b66",
    "resource_az": "br-iaas-odin1a",
    "resource_id": "d6bf7592-ca52-43a2-9979-e418d64b29bb",
    "resource_name": "xzl_ecs-0003-0001",
    "resource_size": 40,
    "resource_type": "OS::Nova::Server",
    "status": "available",
    "updated_at": "2020-08-18T06:06:44.928325",
    "vault_id": "1572bd27-e221-4f28-94ca-9777d232fcd7",
    "replication_records": []
  }
],
"count": 1663
}

```

2. Query backups based on a given resource type.

- API

URI format: GET /v3/{project_id}/backups

The used API is the same as that provided in 1.

- Sample request

GET: https://{endpoint}/v3/0605767b5780d5762fc5c0118072a564/backups?resource_type=OS::Nova::Server&limit=5&offset=0

Obtain the value of **{endpoint}** from [Regions and Endpoints](#).

- Sample response

```

{
  "backups": [
    .....
    {
      "children": [],
      "checkpoint_id": "e328d05e-4b28-4898-b8c1-2bfe6621ec03",
      "created_at": "2020-08-18T07:00:46.932061",
      "description": null,
      "expired_at": null,
      "extend_info": {
        "app_consistency": {
          "app_consistency": "0",
          "app_consistency_status": "0",
          "app_consistency_error_code": "0",
          "app_consistency_error_message": ""
        },
        "auto_trigger": true,
        "bootable": null,
        "os_images_data": null,
        "progress": null,
        "snapshot_id": null,
        "support_llid": false,
        "supported_restore_mode": "backup",
        "system_disk": false,
        "contain_system_disk": true,
        "architecture": "x86_64"
      },
      "id": "c892ed58-3a18-47c2-9e31-a1d543dc490a",
      "image_type": "backup",
      "name": "autobk_7234_0003",
      "parent_id": null,
      "project_id": "0605767b5780d5762fc5c0118072a564",
      "protected_at": "2020-08-18T07:01:12.675112",
      "provider_id": "0daac4c5-6707-4851-97ba-169e36266b66",
      "resource_az": "br-iaas-odin1a",
      "resource_id": "d6bf7592-ca52-43a2-9979-e418d64b29bb",
      "resource_name": "xzl_ecs-0003-0001",
      "resource_size": 40,
    }
  ]
}

```

```
    "resource_type": "OS::Nova::Server",  
    "status": "available",  
    "updated_at": "2020-08-18T07:06:47.518054",  
    "vault_id": "1572bd27-e221-4f28-94ca-9777d232fcd7",  
    "replication_records": []  
  }  
],  
"count": 150  
}
```

6 Permissions Policies and Supported Actions

[6.1 Introduction](#)

[6.2 Category of CBR Actions](#)

6.1 Introduction

You can use Identity and Access Management (IAM) for fine-grained permissions management of your CBR resources. If your cloud account does not need individual IAM users, you can skip this section.

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

You can grant users permissions using roles and policies. Roles are provided by IAM to define service-based permissions that match user's job responsibilities. Policies define API-based permissions for operations on specific resources under certain conditions, allowing for more fine-grained, secure access control of cloud resources.

NOTE

If you want to allow or deny the access to an API, use policy-based authorization.

Each account has all the permissions required to call all APIs, but IAM users must be granted the required permissions. The required permissions are determined by the actions supported by the API. Only users with the policies allowing for those actions can call the API successfully. For example, if an IAM user wants to query ECSs using an API, the user must have been granted permissions that allow the `ecs:servers:list` action.

Supported Actions

CBR provides system-defined policies that can be directly used in IAM. You can also create custom policies to supplement system-defined policies for more refined

access control. Operations supported by policies are specific to APIs. The following are common concepts related to policies:

- Permissions: statements in a policy that allow or deny certain operations
- APIs: REST APIs that can be called by a user who has been granted specific permissions
- Actions: specific operations that are allowed or denied
- Dependencies: actions which a specific action depends on. When allowing an action for a user, you also need to allow any existing action dependencies for that user.
- IAM projects/Enterprise projects: the authorization scope of a custom policy. Policies that contain actions for both IAM and enterprise projects can be used and applied for both IAM and Enterprise Management. Policies that contain actions only for IAM projects can be used and applied to IAM only.

 **NOTE**

The check mark (√) and cross symbol (x) indicate that an action takes effect or does not take effect for the corresponding type of projects.

CBR supports the following actions in custom policies:

- [Example] Vault actions (**Vault**), including all of the actions supported by CBR vault APIs, such as the APIs for creating, modifying, and deleting a vault, querying the vault list, as well as adding and removing resources.
- [Example] Backup sharing actions (**Backup Sharing**), including actions supported by CBR backup sharing APIs, such as APIs for adding share members, obtaining the share member list, and updating the share member status.

6.2 Category of CBR Actions

Task

Permission	API	Action	IAM Project
Querying the task list	GET /v3/{project_id}/operation-logs	cbr:tasks:list	√
Querying a single task	GET /v3/{project_id}/operation-logs/{operation_log_id}	cbr:tasks:get	√

Protection

Permission	API	Action	Related Action	IAM Project
Querying protectable resources	GET /v3/{project_id}/protectables/{protectable_type}/instances	cbr:vaults:listProtectables	ecs:cloudServers:list evs:volumes:list	√
Querying a specified protectable resource	GET /v3/{project_id}/protectables/{protectable_type}/instances/{instance_id}	cbr:vaults:getProtectables	ecs:cloudServers:list evs:volumes:list	√

Vault

Permission	API	Action	Related Action	IAM Project
Applying a policy to a vault	POST /v3/{project_id}/vaults/{vault_id}/associatepolicy	cbr:vaults:associatePolicy	-	√
Querying a specified vault	GET /v3/{project_id}/vaults/{vault_id}	cbr:vaults:get	-	√
Modifying a vault	PUT /v3/{project_id}/vaults/{vault_id}	cbr:vaults:update	-	√
Deleting a vault	DELETE /v3/{project_id}/vaults/{vault_id}	cbr:vaults:delete	-	√
Removing resources	POST /v3/{project_id}/vaults/{vault_id}/removeresources	cbr:vaults:removeResources	-	√

Permission	API	Action	Related Action	IAM Project
Associating resources	POST /v3/{project_id}/vaults/{vault_id}/addresources	cbr:vaults:addResources	ecs:cloudServers:list evs:volumes:list	√
Querying the vault list	GET /v3/{project_id}/vaults	cbr:vaults:list	-	√
Creating a vault	POST /v3/{project_id}/vaults	cbr:vaults:create	ecs:cloudServers:list evs:volumes:list	√
Removing a policy from a vault	POST /v3/{project_id}/vaults/{vault_id}/dissociatepolicy	cbr:vaults:dissociatePolicy	-	√

Restore Point

Permission	API	Action	Related Action	IAM Project
Creating a restore point	POST /v3/{project_id}/checkpoints	cbr:vaults:backup	ecs:cloudServers:list evs:volumes:list	√

Backup Sharing

Permission	API	Action	IAM Project
Adding a share member	POST /v3/{project_id}/backups/{backup_id}/members	cbr:member:create	√
Updating the share member status	PUT /v3/{project_id}/backups/{backup_id}/members/{member_id}	cbr:member:update	√

Permission	API	Action	IAM Project
Querying details about a share member	GET /v3/{project_id}/backups/{backup_id}/members/{member_id}	cbr:member:get	√
Obtaining the share member list	GET /v3/{project_id}/backups/{backup_id}/members	cbr:member:list	√
Deleting a specified share member	DELETE /v3/{project_id}/backups/{backup_id}/members/{member_id}	cbr:member:delete	√

Backup

Permission	API	Action	Related Action	IAM Project
Querying all backups	GET /v3/{project_id}/backups	cbr:backups:list	-	√
Querying a specified backup	GET /v3/{project_id}/backups/{backup_id}	cbr:backups:get	-	√
Deleting a backup	DELETE /v3/{project_id}/backups/{backup_id}	cbr:backups:delete	-	√
Synchronizing a backup	POST /v3/{project_id}/backups/sync	cbr:backups:sync	-	√
Restoring data using a backup	POST /v3/{project_id}/backups/{backup_id}/restore	cbr:backups:restore	ecs:cloudServers:list evs:volumes:list	√

Policy

Permission	API	Action	IAM Project
Querying the policy list	GET /v3/{project_id}/policies	cbr:policies:list	√
Creating a policy	POST /v3/{project_id}/policies	cbr:policies:create	√
Querying a policy	GET /v3/{project_id}/policies/{policy_id}	cbr:policies:get	√
Modifying a policy	PUT /v3/{project_id}/policies/{policy_id}	cbr:policies:update	√
Deleting a policy	DELETE /v3/{project_id}/policies/{policy_id}	cbr:policies:delete	√

7 Appendix

[7.1 Status Codes](#)

[7.2 Error Codes](#)

[7.3 Obtaining a Project ID](#)

7.1 Status Codes

- Normal

Status Code	Description
200 OK	Specifies the normal response code for the GET and PUT operations.
201 Created	Specifies the normal response code for the POST operation.
202 Accepted	The request has been accepted for processing.
204 No Content	Specifies the normal response code for the DELETE operation.

- Abnormal

Status Code	Description
400 Bad Request	The server failed to process the request.
401 Unauthorized	You need to enter the username and password to access the requested page.
403 Forbidden	Access to the requested page is forbidden.
404 Not Found	The server could not find the requested page.

Status Code	Description
405 Method Not Allowed	The method specified in the request is not allowed.
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	The request is not completed because of a service error.
501 Not Implemented	The request is not completed because the server does not support the requested function.
502 Bad Gateway	The request is not completed because the server receives an invalid request.
503 Service Unavailable	The request is not completed because the service is unavailable.
504 Gateway Timeout	A gateway timeout error occurs.

7.2 Error Codes

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.0001	No resource is available for backup.	No resource is available for backup.	Check whether resources are being backed up or contact technical support.
400	BackupService.1011	The destination project does not support replication.	The destination project does not support replication.	Contact technical support.

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.2001	Restoration cannot be executed because the size of the disk on the server is smaller than the backup size.	Restoration cannot be executed because the size of the disk on the server is smaller than the backup size.	Perform the operation according to the constraints.
400	BackupService.2002	The resource is being backed up. Restore the resource after the backup is complete.	The resource is being backed up. Restore the resource after the backup is complete.	Perform the operation according to the constraints.
400	BackupService.2003	Restoration to a different server is not allowed.	Restoration to a different server is not allowed.	Perform the operation according to the constraints.
400	BackupService.2005	Restoration is not allowed in the current backup status.	Restoration is not allowed in the current backup status.	Perform the operation according to the constraints.
400	BackupService.2007	A terminated ECS cannot be restored.	A terminated ECS cannot be restored.	Ensure that the ECS status is available and then perform backups.
400	BackupService.2008	Restoration is not allowed in the current ECS status.	Restoration is not allowed in the current ECS status.	Check the ECS status.
400	BackupService.2009	Restoration is not allowed in the current disk type.	Restoration is not allowed in the current disk type.	Perform the operation according to the constraints.
400	BackupService.2010	The resource is being restored.	The resource is being restored.	Try again later.
400	BackupService.2011	Restoration is not allowed in the current disk status.	Restoration is not allowed in the current disk status.	Check the disk status.

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.2012	Restoration of some disks is not allowed.	Restoration of some disks is not allowed.	Contact technical support.
400	BackupService.2013	Backup data of a data disk cannot be restored to a system disk.	Backup data of a data disk cannot be restored to a system disk.	Use valid values for restoration parameters.
400	BackupService.2014	A BMS backup cannot be restored to an ECS.	A BMS backup cannot be restored to an ECS.	Select a proper backup for restoration.
400	BackupService.2015	Restoration is not allowed between different architectures.	Restoration is not allowed between different architectures.	Select a proper architecture for restoration.
400	BackupService.6001	The maximum number of this type of policies has been reached.	The maximum number of this type of policies has been reached.	Contact technical support.
400	BackupService.6003	The destination region cannot be changed because the policy has been applied to a replication vault.	The destination region cannot be changed because the policy has been applied to a replication vault.	Remove the policy from the vault and try again.
400	BackupService.6100	The maximum number of vault resources has been reached.	The maximum number of vault resources has been reached.	Create a new vault and associate resources with the new vault.
400	BackupService.6101	Invalid vault capacity.	Invalid vault capacity.	Use valid values for vault parameters.
400	BackupService.6102	The vault does not support this resource type.	The vault does not support this resource type.	Use valid values for vault type parameters.

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.6103	The resource has been associated with a vault.	The resource has been associated with a vault.	Use valid values for resource parameters.
400	BackupService.6104	Duplicate vault resources.	Duplicate vault resources.	Use valid values for resource parameters.
400	BackupService.6106	The vault already exists.	The vault already exists.	Use valid values for vault parameters.
400	BackupService.6107	Vault capacity expansion failed.	Vault capacity expansion failed.	Try again. If the fault persists, contact technical support.
400	BackupService.6108	New resources cannot be associated with the vault.	New resources cannot be associated with the vault.	Try again. If the fault persists, contact technical support.
400	BackupService.6109	The bill does not exist.	The bill does not exist.	Contact technical support.
400	BackupService.6110	The vault cannot be updated.	The vault cannot be updated.	Try again. If the fault persists, contact technical support.
400	BackupService.6111	The vault cannot be deleted.	The vault cannot be deleted.	Try again. If the fault persists, contact technical support.
400	BackupService.6112	Invalid vault status.	Invalid vault status.	Perform the operation in the correct status.
400	BackupService.6113	Backup is not allowed in the current vault status.	Backup is not allowed in the current vault status.	Perform the operation in the correct status.
400	BackupService.6114	The used capacity of the vault exceeds the maximum capacity.	The used capacity of the vault exceeds the maximum capacity.	Use vaults properly.

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.6115	Failed to delete the backups of vault resources.	Failed to delete the backups of vault resources.	Try again. If the fault persists, contact technical support.
400	BackupService.6116	Unsupported resource type.	Unsupported resource type.	Enter a valid protect type value.
400	BackupService.6117	Unknown policy type.	Unknown policy type.	Enter a valid OperationType value.
400	BackupService.6118	Failed to check the destination vault.	Failed to check the destination vault.	Try again. If the fault persists, contact technical support.
400	BackupService.6119	The destination vault does not support replication.	The destination vault does not support replication.	Check whether the destination vault supports replication.
400	BackupService.6120	The destination vault does not exist.	The destination vault does not exist.	Check whether the destination vault exists.
400	BackupService.6121	Vault deletion failed.	Vault deletion failed.	Try again. If the fault persists, contact technical support.
400	BackupService.6122	The resource type does not support replication.	The resource type does not support replication.	Check whether the resource type supports replication.
400	BackupService.6123	Capacity expansion failed. There may be unprocessed capacity expansion orders or capacity expansion is in progress.	Capacity expansion failed. There may be unprocessed capacity expansion orders or capacity expansion is in progress.	Try again. If the fault persists, contact technical support.

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.6124	Backup is not allowed for the current type of vaults.	Backup is not allowed for the current type of vaults.	Use different types of vaults properly.
400	BackupService.6125	A backup task is in progress.	A backup task is in progress.	Perform backups after the current backup task is complete.
400	BackupService.6126	Database backup is not allowed for this vault.	Database backup is not allowed for this vault.	Use different types of vaults properly.
400	BackupService.6127	This policy cannot be applied to this vault.	This policy cannot be applied to this vault.	Use different types of vaults properly.
400	BackupService.6128	Replication is not allowed for the current type of vaults.	Replication is not allowed for the current type of vaults.	Use a proper type of vault for replication.
400	BackupService.6129	The maximum capacity of the destination vault has been reached.	The maximum capacity of the destination vault has been reached.	Expand the vault capacity and then perform this operation.
400	BackupService.6130	The vault is being replicated.	The vault is being replicated.	Try again later.
400	BackupService.6131	The traffic record does not exist.	The traffic record does not exist.	Contact technical support.
400	BackupService.6133	The maximum number of vaults has been reached.	The maximum number of vaults has been reached.	Contact technical support.
400	BackupService.6134	Resources are being removed from the vault.	Resources are being removed from the vault.	Try again later.
400	BackupService.6135	The resource does not exist in the vault.	The resource does not exist in the vault.	Check whether the resource has been associated with the vault.

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.6136	Backup policies cannot be applied with hybrid cloud backup vaults.	Backup policies cannot be applied with hybrid cloud backup vaults.	Contact technical support.
400	BackupService.6140	An encrypted disk cannot be specified as a system disk.	An encrypted disk cannot be specified as a system disk.	Perform the operation according to the constraints.
400	BackupService.6141	A SCSI disk cannot be specified as a system disk.	A SCSI disk cannot be specified as a system disk.	Perform the operation according to the constraints.
400	BackupService.6142	Maximum capacities of all vaults have been reached.	Maximum capacities of all vaults have been reached.	Expand vault capacities and try again.
400	BackupService.6201	The backup cannot be deleted.	The backup cannot be deleted.	Try again. If the fault persists, contact technical support.
400	BackupService.6202	Backups can be used for restoration only when the vault status is Available.	Backups can be used for restoration only when the vault status is Available.	Perform the operation in the correct status.
400	BackupService.6203	Performing backups.	Performing backups.	Perform backups after the current task is complete.
400	BackupService.6204	The backup cannot be deleted because it has been used to create an image.	The backup cannot be deleted because it has been used to create an image.	Delete the created image and then delete the backup.
400	BackupService.6206	Metadata query is not allowed in the current backup status.	Metadata query is not allowed in the current backup status.	Try again later.

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.6215	Backup is not allowed in the current resource status.	Backup is not allowed in the current resource status.	Check whether the resource can be backed up in the current status.
400	BackupService.6216	The backup cannot be deleted because it is in use.	The backup cannot be deleted because it is in use.	Try again later.
400	BackupService.6300	The resource type and backup provider do not match.	The resource type and backup provider do not match.	Contact technical support.
400	BackupService.6301	Invalid backup provider ID.	Invalid backup provider ID.	Use a valid provider ID.
400	BackupService.6400	Bucket creation failed.	Bucket creation failed.	Try again. If the fault persists, contact technical support.
400	BackupService.6401	Failed to set the bucket quota.	Failed to set the bucket quota.	Try again. If the fault persists, contact technical support.
400	BackupService.6403	Failed to obtain bucket storage information.	Failed to obtain bucket storage information.	Try again. If the fault persists, contact technical support.
400	BackupService.6404	Bucket deletion failed.	Bucket deletion failed.	Try again. If the fault persists, contact technical support.
400	BackupService.6405	Bucket object deletion failed.	Bucket object deletion failed.	Try again. If the fault persists, contact technical support.
400	BackupService.6406	Failed to list bucket objects.	Failed to list bucket objects.	Try again. If the fault persists, contact technical support.

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.6407	Failed to set the bucket ACL.	Failed to set the bucket ACL.	Try again. If the fault persists, contact technical support.
400	BackupService.6408	Failed to set the bucket policy.	Failed to set the bucket policy.	Try again. If the fault persists, contact technical support.
400	BackupService.6600	The maximum number of tags has been reached for the resource.	The maximum number of tags has been reached for the resource.	Delete some tags and try again.
400	BackupService.6700	Only cloud server backups can be shared.	Only cloud server backups can be shared.	Share cloud server backups.
400	BackupService.6701	The maximum number of backups that can be shared has been reached.	The maximum number of backups that can be shared has been reached.	Check whether the maximum number of backups that can be shared has been reached.
400	BackupService.6702	Only backups in the Available status can be shared.	Only backups in the Available status can be shared.	Share backups that are in the Available status.
400	BackupService.6703	The backup has been shared.	The backup has been shared.	Check whether the backup has already been shared to a user.
400	BackupService.6704	Invalid project ID of the tenant for sharing.	Invalid project ID of the tenant for sharing.	Use a correct project ID for sharing.
400	BackupService.6706	Invalid update parameter value for the share member.	Invalid update parameter value for the share member.	Use valid values for update parameters.
400	BackupService.6707	Backup sharing is not allowed.	Backup sharing is not allowed.	Check whether backup sharing is supported.

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.6708	Failed to update the status of a share member.	Failed to update the status of a share member.	Contact technical support.
400	BackupService.6709	Backup sharing is not allowed for cloud servers using encrypted disks.	Backup sharing is not allowed for cloud servers using encrypted disks.	Perform the operation according to the constraints.
400	BackupService.6710	The shared backup has been used to register an image.	The shared backup has been used to register an image.	Delete the image first.
400	BackupService.6711	Shared backup deletion failed.	Shared backup deletion failed.	Contact technical support.
400	BackupService.6712	Backup sharing is not allowed in the current vault status.	Backup sharing is not allowed in the current vault status.	Perform the operation according to the constraints.
400	BackupService.6713	The type of the vault accepting the shared backup and the backup resource type are different.	The type of the vault accepting the shared backup and the backup resource type are different.	The vault type and resource type must be the same.
400	BackupService.6714	A shared backup cannot be shared to the same member again.	A shared backup cannot be shared to the same member again.	Perform the operation according to the constraints.
400	BackupService.7001	DESS disks cannot be backed up.	DESS disks cannot be backed up.	Perform the operation according to the constraints.

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.7002	SCSI disks cannot be backed up.	SCSI disks cannot be backed up.	Perform the operation according to the constraints.
400	BackupService.7003	Backup is not allowed in the current disk status.	Backup is not allowed in the current disk status.	Perform the operation in the correct status.
400	BackupService.7004	Backup or restoration is not allowed for this disk.	Backup or restoration is not allowed for this disk.	Contact technical support.
400	BackupService.7006	The disk already exists in the vault.	The disk already exists in the vault.	Dissociate the disk from the vault and then perform this operation.
400	BackupService.7007	A disk created a long time ago cannot be backed up.	A disk created a long time ago cannot be backed up.	Replace the disk and perform backups.
400	BackupService.7008	Disks at the disaster recovery site cannot be restored.	Disks at the disaster recovery site cannot be restored.	Perform the operation in the correct status.
400	BackupService.7101	Backup is not allowed in the current server status.	Backup is not allowed in the current server status.	Perform the operation in the correct status.
400	BackupService.7102	The server has stopped.	The server has stopped.	Perform the operation in the correct status.
400	BackupService.7103	The server cannot be backed up.	The server cannot be backed up.	Contact technical support.
400	BackupService.7104	Backup is not allowed for servers using SCSI disks.	Backup is not allowed for servers using SCSI disks.	Detach the SCSI disks and then perform backups.
400	BackupService.7105	Inconsistent disk backends.	Inconsistent disk backends.	Contact technical support.

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.7106	Shared disks cannot be backed up.	Shared disks cannot be backed up.	Perform the operation according to the constraints.
400	BackupService.7107	The maximum number of shared disks has been reached.	The maximum number of shared disks has been reached.	Exclude the shared disks and then perform backups.
400	BackupService.7108	Backup is not allowed for servers containing no disks.	Backup is not allowed for servers containing no disks.	Attach disks to the server and then perform backups.
400	BackupService.7109	BMSs cannot be backed up.	BMSs cannot be backed up.	Perform the operation according to the constraints.
400	BackupService.7110	The resource type and provider ID do not match.	The resource type and provider ID do not match.	Use a valid provider ID.
400	BackupService.7111	Backup is not allowed for servers using DESS disks.	Backup is not allowed for servers using DESS disks.	Detach DESS disks and then perform backups.
400	BackupService.7113	BMS local disks cannot be backed up.	BMS local disks cannot be backed up.	Exclude local disks and then perform backups.
400	BackupService.7114	Restoration to the source server running a different operating system is not allowed.	Restoration to the source server running a different operating system is not allowed.	Use valid values for restoration parameters.
400	BackupService.7115	The backup server and the destination server to be restored have different types.	The backup server and the destination server to be restored have different types.	Use valid values for restoration parameters.

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.7116	The server has been associated with the vault.	The server has been associated with the vault.	Dissociate the server from the vault and then perform this operation.
400	BackupService.7117	Restoration is not allowed for disaster recovery site servers.	Restoration is not allowed for disaster recovery site servers.	Use valid values for restoration parameters.
400	BackupService.7200	Cloud databases are being backed up.	Cloud databases are being backed up.	Try again later.
400	BackupService.7201	The disk is not attached to any server.	The disk is not attached to any server.	Confirm and then try again.
400	BackupService.7203	The snapshot is not in the correct status.	The snapshot is not in the correct status.	Try again later.
400	BackupService.7204	The snapshot and disk do not match.	The snapshot and disk do not match.	Confirm and then try again.
400	BackupService.7300	The vault does not support synchronization.	The vault does not support synchronization.	Check whether the vault type supports synchronization.
400	BackupService.7301	The vault is not empty.	The vault is not empty.	Perform the operation according to the constraints.
400	BackupService.7302	Backups are being synchronized.	Backups are being synchronized.	Perform the operation according to the constraints.
400	BackupService.7303	The maximum number of vaults has been reached.	The maximum number of vaults has been reached.	Contact technical support.

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.7501	SFS Turbo file systems are being backed up.	SFS Turbo file systems are being backed up.	Try again later.
400	BackupService.7502	Backup is not allowed in the current status of the SFS Turbo file system.	Backup is not allowed in the current status of the SFS Turbo file system.	Perform the operation in the correct status.
400	BackupService.7503	Backup is not allowed in the current sub-status of the SFS Turbo file system.	Backup is not allowed in the current sub-status of the SFS Turbo file system.	Perform the operation in the correct status.
400	BackupService.7504	Failed to freeze the SFS Turbo file system.	Failed to freeze the SFS Turbo file system.	Try again later.
400	BackupService.7505	Failed to unfreeze the SFS Turbo file system.	Failed to unfreeze the SFS Turbo file system.	Try again later.
400	BackupService.7506	Failed to execute tasks of the SFS Turbo file system.	Failed to execute tasks of the SFS Turbo file system.	Try again later or contact technical support.
400	BackupService.7507	Restoration is not allowed because the SFS Turbo file system is different from when it is backed up.	Restoration is not allowed because the SFS Turbo file system is different from when it is backed up.	Perform the operation in the correct status.
400	BackupService.7508	SFS Turbo file system pre-restoration failed.	SFS Turbo file system pre-restoration failed.	Try again. If the fault persists, contact technical support.

Status Code	Error Code	Error Message	Description	Handling Measure
400	BackupService.7509	SFS Turbo file system restoration failed.	SFS Turbo file system restoration failed.	Try again. If the fault persists, contact technical support.
400	BackupService.7510	SFS Turbo backups can only be restored to original SFS Turbo file systems.	SFS Turbo backups can only be restored to original SFS Turbo file systems.	Restore to the original SFS Turbo file system.
400	BackupService.7511	Restoration is not allowed in the current status of the SFS Turbo file system.	Restoration is not allowed in the current status of the SFS Turbo file system.	Perform the operation in the correct status.
400	BackupService.8300	Insufficient snapshot quota.	Insufficient snapshot quota.	Increase quota and then try again.
400	BackupService.9900	Parameter verification failed.	Parameter verification failed.	Use valid parameter values.
403	BackupService.8600	Not authenticated.	Not authenticated.	Complete real-name authentication.
404	BackupService.4001	The migration record does not exist.	The migration record does not exist.	Provide a correct migration record ID.
404	BackupService.6000	The policy does not exist.	The policy does not exist.	Check whether the policy exists.
404	BackupService.6002	The vault is not applied with the policy.	The vault is not applied with the policy.	Apply the backup policy to the vault first.
404	BackupService.6105	The vault does not exist.	The vault does not exist.	Use valid values for vault parameters.
404	BackupService.6200	The backup does not exist.	The backup does not exist.	Check whether the backup exists.

Status Code	Error Code	Error Message	Description	Handling Measure
404	BackupService.6217	The backup restore point does not exist.	The backup restore point does not exist.	Check whether the backup restore point exists.
404	BackupService.6302	The resource does not exist.	The resource does not exist.	Confirm the queried resource.
404	BackupService.6402	The bucket is not empty.	The bucket is not empty.	Delete backups and backup policies to empty the bucket.
404	BackupService.6500	The operation log does not exist.	The operation log does not exist.	Check whether the respective task exists.
404	BackupService.6501	The task does not exist.	The task does not exist.	Check whether the task exists.
404	BackupService.6601	The key does not exist.	The key does not exist.	Enter a correct key.
404	BackupService.6705	The share member does not exist.	The share member does not exist.	Check whether the share member exists.
404	BackupService.7000	The disk does not exist.	The disk does not exist.	Perform the operation according to the constraints.
404	BackupService.7100	The server does not exist.	The server does not exist.	Perform the operation in the correct status.
404	BackupService.7202	Failed to obtain the snapshot.	Failed to obtain the snapshot.	Confirm the query parameters.
404	BackupService.7500	The SFS Turbo file system does not exist.	The SFS Turbo file system does not exist.	Checks whether the SFS Turbo file system exists.
500	BackupService.0002	Resources are being backed up.	Resources are being backed up.	Try again later.
500	BackupService.1005	The destination region does not support replication.	The destination region does not support replication.	Check whether the current region supports replication.

Status Code	Error Code	Error Message	Description	Handling Measure
500	BackupService.1006	Failed to import the backup replica.	Failed to import the backup replica.	Contact technical support.
500	BackupService.4004	Failed to clean up data.	Failed to clean up data.	Try again later.
500	BackupService.4005	Failed to check the destination vault.	Failed to check the destination vault.	Try again later.
500	BackupService.4006	Failed to migrate the backup in an intermediate status.	Failed to migrate the backup in an intermediate status.	Try again later.
500	BackupService.4007	Failed to check the migration progress of other regions.	Failed to check the migration progress of other regions.	Try again later.
500	BackupService.6132	Vault creation failed.	Vault creation failed.	Try again. If the fault persists, contact technical support.
500	BackupService.6137	One disk on cloud servers cannot be backed up in multiple vaults.	One disk on cloud servers cannot be backed up in multiple vaults.	Associate servers using the same disk to the same vault.
500	BackupService.6138	Failed to obtain language preferences from CBC.	Failed to obtain language preferences from CBC.	Only Chinese and English are supported.
500	BackupService.6139	Failed to obtain xdomain_type .	Failed to obtain xdomain_type .	Try again later.

Status Code	Error Code	Error Message	Description	Handling Measure
500	BackupService.6207	This type of backups cannot be used to create images.	This type of backups cannot be used to create images.	Perform the operation according to the constraints.
500	BackupService.6208	Image creation is not allowed in the current backup status.	Image creation is not allowed in the current backup status.	Try again later or contact technical support.
500	BackupService.6209	The backup does not contain the system disk data and cannot be used to create an image.	The backup does not contain the system disk data and cannot be used to create an image.	Perform the operation according to the constraints.
500	BackupService.6210	An image has been created using the backup.	An image has been created using the backup.	Perform the operation according to the constraints.
500	BackupService.6211	An image has been created using the backup.	An image has been created using the backup.	Perform the operation according to the constraints.
500	BackupService.6212	Image creation failed.	Image creation failed.	Contact technical support.
500	BackupService.6213	The backup and the image do not match.	The backup and the image do not match.	Contact technical support.
500	BackupService.6214	Failed to deregister the image.	Failed to deregister the image.	Contact technical support.
500	BackupService.7009	The disk backup is being lazyloaded after deleted.	The disk backup is being lazyloaded after deleted.	Perform the operation in the correct status.
500	BackupService.8400	Failed to obtain the product from CBC.	Failed to obtain the product from CBC.	Try again later.

Status Code	Error Code	Error Message	Description	Handling Measure
500	BackupService.9910	Unknown error.	Unknown error.	Contact technical support.
500	BackupService.9998	Authentication failed.	Authentication failed.	Confirm user information.

7.3 Obtaining a Project ID

Scenarios

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

- [Obtain the Project ID by Calling an API](#)
- [Obtain the Project ID from the Console](#)

Obtain the Project ID by Calling an API

You can obtain the project ID by calling the IAM API used to query project information based on the specified criteria.

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

The following is an example response. The value of **id** is the project ID.

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

Obtain a Project ID from the Console

To obtain a project ID from the console, perform the following operations:

1. Log in to the management console.
2. Click the username and select **My Credentials** from the drop-down list.
On the **My Credentials** page, view the project ID (value in the **Project ID** column).

A Change History

Released On	Description
2021-09-30	This issue is the third official release, which incorporates the following change: Added descriptions of permission management.
2021-02-08	This issue is the second official release, which incorporates the following change: Added support for SFS Turbo file system backup.
2020-02-26	This issue is the first official release.