

# Alibaba Cloud Hybrid Backup

Back up CSG

Issue: 20190802

## Legal disclaimer

---

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use








or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.



## Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 <b>Danger:</b> Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 <b>Warning:</b> Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 <b>Notice:</b> Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click OK.
<code>Courier</code> font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[ ] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand   slave}</code>



# Contents

---

Legal disclaimer.....	I
Generic conventions.....	I
1 Overview.....	1
2 Preparations.....	2
3 Back up a CSG instance.....	5
4 Restore a CSG instance.....	8
5 Configure the backup alarm function.....	9
6 Create and use a mirror vault.....	13



# 1 Overview

---

Hybrid Backup Recovery (HBR) is a fully managed online backup service that allows you to back up data to the cloud in an efficient, secure, and cost-effective way. You can use the Storage Gateway Backup service provided by HBR to back up Cloud Storage Gateway (CSG) instances.

For more information about how to back up CSG instances, see the following topics:

- [Preparations](#)
- [Back up a CSG instance](#)
- [Restore a CSG instance](#)

For more information about other features of the Storage Gateway Backup service, see the following topics:

- [Configure the backup alarm function](#)
- [Create and use a mirror vault](#)

## 2 Preparations

---

You can use HBR to back up CSG instances and restore them when necessary. This topic describes the preparations that you need to make before backing up data.


### Activate a RAM user

Resource Access Management (RAM) is an Alibaba Cloud service that helps you manage user identities and access to your cloud resources. You can create and manage multiple RAM users within a single Alibaba Cloud account. You can grant different permissions to each RAM user, so that RAM users have different access permissions on Alibaba Cloud resources. Make sure that you have [Created a RAM user](#) and [Created an access key for a RAM user](#) before backing up data.

### Register a CSG instance

1. Log on to the [HBR console](#).
2. Select the region of the CSG instance to be backed up.
3. In the left-side navigation pane, click Storage Gateway Backup.
4. On the Storage Gateway Backup page, click Register Cloud Gateway in the upper-right corner.


5. In the Register Cloud Gateway dialog box that appears, set the parameters as instructed in the following table.

Parameter	Description
Backup Vault Name	<p>Specify the backup vault. A backup vault is a repository used by HBR to store backup data on the cloud. You can back up data from multiple clients to the same vault.</p> <ul style="list-style-type: none"><li>· If you have created backup vaults: Click Select Vault and select a vault from the drop-down list.</li><li>· If you have not created any backup vaults: Click Create Vault, and enter the vault name and description to create a vault. The vault name must not exceed 64 bytes in length.</li></ul>
Cloud Gateway Cluster	Select the gateway cluster of the CSG instance to be backed up.
Please select a cloud gateway to backup	<p>Select the CSG instance to be backed up.</p> <div> <b>Note:</b> The Storage Gateway Backup service can only back up standard or enhanced file gateways on Alibaba Cloud.</div>

6. After the configuration is completed, click Create. The system automatically installs the backup client for the CSG instance on the corresponding ECS instance.

#### Manage clients of CSG instances

On the Storage Gateway Backup page, click the Cloud Gateway Instance tab, and then locate the target CSG instance.

Operation	Procedure
To check the installation status of a client	<p>Make sure that the client status appears as <b>Activated</b> after the client is installed.</p> <p>If the status is <b>Failed</b> , follow the instructions provided in the error message for troubleshooting. After the error is rectified, choose <b>More &gt; Re-install</b> in the <b>Actions</b> column.</p>
To uninstall a client	Choose <b>More &gt; Uninstall Client</b> in the <b>Actions</b> column.
To delete a client and the corresponding CSG instance	<p>Choose <b>More &gt; Delete</b> in the <b>Actions</b> column.</p> <div> <b>Note:</b> Before deleting a client, make sure that the client has no backup job in the <b>Running</b> or <b>Completed</b> status.</div>

## 3 Back up a CSG instance

---

You can use HBR to back up CSG instances. When any file gateway is lost or damaged, you can restore it by using a backup. This topic describes how to back up a CSG instance.

### Prerequisites

You have completed [preparations](#).

### Procedure

1. Log on to the [HBR console](#).
2. Select the region of the CSG instance to be backed up.
3. In the left-side navigation pane, click Storage Gateway Backup.
4. On the Storage Gateway Backup page, click the Cloud Gateway Instance tab.
5. Locate the target CSG instance and click Backup in the Actions column.
6. In the Select Backup Source step in the Create Backup Plan wizard, select the shared data source of the CSG instance to be backed up. Click Next.
7. In the Config Backup Plan step, set the parameters as instructed in the following table, and then click Create.


Parameter	Description
Source Path	<ul style="list-style-type: none"><li>• The path of the backup source. You can enter a maximum of eight source paths, which means that you can back up files from eight directories at a time.</li><li>• The source path must be an absolute path.</li><li>• You can enter a Uniform Naming Convention (UNC) path as a source path.</li><li>• Separate multiple source paths with carriage returns.</li></ul>
Plan Name	The name of the backup plan. If you leave this field blank, a random name is specified by default.

Parameter	Description
Retention	The retention period of the backup. Valid units: day, week, month, and year.
Start Time	The start time of the backup plan. The time is accurate to the second.
Plan Interval	The frequency of incremental backups. Valid units: hour, day, and week.
Using Flow Control	You can enable throttling to set bandwidth limits for backing up data from a directory during peak hours. This ensures business continuity. If you select Use, select a throttling period and enter the maximum bandwidth that can be used for backup in the throttling period based on business requirements, and then click Add.

#### Related operations

On the Storage Gateway Backup page, click the Backup Plan and Job tab, where you can perform the operations as described in the following table.

Operation	Procedure
To view an error report	Locate the target backup plan and view the backup progress in the Status column. If some files fail to be backed up, click View next to the backup plan in the Actions column. Then, click the Download icon in Errors column to download the error report.
To start a backup job	In the Actions column of the target backup plan, choose More > Execute Now.
To cancel a running backup job	In the Actions column of the target backup plan, choose More > Cancel Task.
To pause a running backup job	In the Actions column of the target backup plan, choose More > Pause.
To resume a paused backup job	In the Actions column of the target backup plan, choose More > Enable.

Operation	Procedure
To modify a backup plan	In the Actions column of the target backup plan, choose More > Edit.
To delete a backup plan	<div>In the Actions column of the target backup plan, choose More &gt; Delete.</div> <div> <b>Note:</b> After you delete a backup plan, it no longer runs. However, data that you have backed up by using the plan is retained.</div>

## 4 Restore a CSG instance

---

You can restore a file gateway backup to its original CSG instance. When necessary, you can also restore the file gateway backup of a CSG instance to another CSG instance in the same vault.

### Procedure

1. Log on to the [HBR console](#).
2. Select the region of the CSG instance to which you want to restore data.
3. In the left-side navigation pane, click Storage Gateway Backup.
4. On the Storage Gateway Backup page, click the Cloud Gateway Instance tab.
5. Locate the target CSG instance and click Restore in the Actions column.
6. In the Select Source Instance step in the New Restore Task wizard, set Restore Resource as needed.

- From This ECS

Select this option if you need to restore backup files from the current CSG instance. Then, perform the following steps:

- a. Click Next.
- b. In the Select Snapshot step, select a snapshot and click Next.
- c. In the Config Restore Rules step, enter the path to restore data, select the files to be restored, and then click Create.

- From Other ECS

Select this option if you need to restore backup files from another CSG instance in the same vault to the current CSG instance. Then, perform the following steps:

- a. Select the CSG instance where the backup files reside and click Next.
- b. In the Select Snapshot step, select a snapshot and click Next.
- c. In the Config Restore Rules step, enter the path to restore data, select the files to be restored, and then click Create.

### Related operations

On the Storage Gateway Backup page, click the Restore Jobs tab. On this tab, you can view the restoration status of a job or cancel a running job.



## 5 Configure the backup alarm function

---

If a backup fails or a client is disconnected from a server, HBR sends alarm SMS messages or emails to your Alibaba Cloud account by default. You can customize the alarm policy and the contact or contact group to receive alarms.

### Context



#### Note:

The specified contact or contact group receives an alarm after a backup fails or a client is disconnected from a server for about an hour.

### Create an alarm contact

An alarm contact is a person that is assigned to receive backup alerts. You can create an alarm contact as follows:

1. Log on to the [Hybrid Backup Recovery \(HBR\) console](#).
2. In the left-side navigation pane, select Alarm Contact.
3. On the Alarm Contact Management page, select the Alarm Contact tab.
4. Click New Contact in the upper-right corner.
5. In the New Contact dialog box, enter the Contact Name .
6. Select a Contact Method , and then perform the following steps.

- Email

If you select Email as a contact method, enter the Contact Email, and then click Send Verification. Log on to the specified email to view the verification code, go back to the HBR console, and enter the verification code in the Email Verification field.

- Mobile

If you select Mobile as a contact method, enter the Mobile and then click Send Verification. An SMS message that contains a verification code will be sent to your mobile phone. Enter the verification code in the Mobile Verification Code field.


7. Click OK.

**Note:**

- On the Alarm Contact tab, you can view a list of all contacts and the related information of each contact.
- You can click Edit to modify the email and mobile number.
- You cannot delete a contact that is selected to receive alerts or added to a contact group.

### Create an alarm contact group

If you need multiple contacts to receive alerts, you can create an alarm contact group and add these contacts to the contact group to facilitate management. When an alert occurs, all contacts that are included in a contact group will receive an alert.

1. Log on to the [HBR console](#).
2. In the left-side navigation pane, select Alarm Contact.
3. On the Alarm Contact Management page, select the Alarm Contact Group tab.
4. In the upper-right corner, click New Contact Group.
5. In the New Contact Group dialog box, enter the Group Name .
6. Select one or more contacts, and click the  icon to add the contact to the group. These contacts are displayed in the Selected Contacts area.
7. Click OK.

**Note:**

- On the Alarm Contact Group tab, you can view a list of all contact groups and the number of contacts in each group.
- You can click Edit to modify a contact group.
- You cannot delete a contact group that is selected to receive alerts.

### Customize a backup alarm policy

You can customize the following types of backup alarm policies:

**Note:**

HBR sends alarm SMS messages or emails to your Alibaba Cloud account by default. If you customize a vault-level alarm policy and an instance-level alarm policy, the instance-level alarm policy takes precedence over the vault-level alarm policy.

- Vault-level alarm policies

A vault-level alarm policy applies to all the backup clients of a vault. The backup clients include those installed on ECS instances, local hosts, and local virtual machines.

- Instance-level alarm policies

An instance-level alarm policy applies to the backup client installed on a specific instance.

### Vault-level alarm policy

The procedure is as follows:

1. Log on to the [HBR console](#).
2. On the Overview page, locate the vault for which you need to create an alarm policy.
3. In the upper-right corner of a vault card, click Settings.
4. On the Vault Setting page, select an Alarm Policy as required.

- Disabled

After you select this option, no alert is sent when an alarm occurs on a backup client or instance that is related to the vault.

- Default Notification

After you select this option, alerts for the vault are sent to an Alibaba Cloud account by using SMS messages and emails.

- Customized Notification

After you select this option, you can select one or more contacts, and contact groups. After you complete the configuration, alert for the vault are sent to the selected contacts or contact groups.

5. Click OK.

### Instance-level alarm policy

The procedure is as follows:

1. Log on to the [HBR console](#).

2. Select the region of the CSG instance for which you want to customize an instance-level alarm policy.
3. In the left-side navigation pane, click Storage Gateway Backup.
4. On the Storage Gateway Backup page, click the Cloud Gateway Instance tab.
5. Locate the target CSG instance and choose More > Alarm Setting in the Actions column.
6. In the Alarm Policy dialog box that appears, specify the alarm policy as needed.

Alarm Policy	Description
Disabled	If you select this option, no alert is sent when an alarm occurs on the instance.
Same as Vault	If you select this option, the alarm policy of the vault where the ECS instance is located applies to the instance.
Default Notification	If you select this option, alerts for the instance are sent to an Alibaba Cloud account by using SMS messages and emails.
Customized Notification	You can select one or more contacts and contact groups. After you complete the configuration, alerts for the instance are set to the selected contacts or contact groups.

7. Click Ok.

## 6 Create and use a mirror vault

---

A backup vault is a repository used by HBR to store backup data on the cloud.

You can create a remote mirror vault for a backup vault to meet disaster recovery requirements. When necessary, you can use the remote mirror vault for cross-region data restoration.




### Note:

- After a mirror vault is created, data that is being backed up by a backup job in the source vault is synchronized to the mirror vault in real time. The historical backups stored in the source vault start being synchronized to a mirror vault 90 minutes after the creation of the mirror vault.
- You can only create one mirror vault for each backup vault.
- You can restore backups stored in a mirror vault but cannot back up data to a mirror vault.
- You must delete a mirror vault before deleting its source vault.
- A source vault is created when you create a backup client.

### Create a mirror vault

Proceed as follows:

1. Log on to the [HBR console](#).
2. In the left-side navigation pane, select Overview.
3. Locate a vault for which you want to create a mirror vault, click the  icon in the upper-right corner.
4. In the Create Mirror Vault dialog box, select a region where the new mirror vault is located.



### Note:

For disaster recovery, you cannot select the region where the source vault is located.

5. Enter the Vault Name . The name must be a maximum of 32 characters in length.
6. Enter the Vault Description as required, and click Create.

## Restore backup data from a mirror vault

After a mirror vault is created, you can use it to restore backup data when necessary.

The procedure is as follows:

1. Log on to the [HBR console](#).
2. Select the region of the mirror vault and [register a CSG instance](#) for the mirror vault.
3. Locate the target CSG instance and use it to [restore backup data](#).



### Note:

You must set `Restore Resource` to `From Other ECS`.