ALIBABA CLOUD

Alibaba Cloud

Hybrid Backup

Back up CSG

Document Version: 20200922

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Overview ---- 05
2.Preparations ---- 06
3.Back up shares of a gateway ---- 08
4.Restore shares of a gateway ---- 11
5.Configure alert notifications ---- 12
6.Restore shares across regions by using a mirror vault ---- 15

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 CSG backup service to back up shares of Cloud Storage Gateway (CSG).

You can use the following procedure to back up shares of gateways:

- Preparations
- Back up shares of a gateway
- Restore shares of a gateway

For more information about other features of CSG backup, see the following topics:

- Configure alert notifications
- Restore shares across regions by using a mirror vault

2.Preparations

You can use Hybrid Backup Recovery (HBR) to back up shares of Cloud Storage Gateway (CSG). You can then restore the shares if needed. This topic describes the preparations that you must make before backup.

> **Note** You can use the CSG backup service in the following regions: China (Shanghai), China (Hangzhou), China (Beijing), China (Shenzhen), China (Zhangjiakou-Beijing Winter Olympics), China (Hohhot), China (Hong Kong), Singapore (Singapore), Australia (Sydney), US (Silicon Valley), and Japan (Tokyo). This service will be available in more regions soon.

(Recommended) Prepare an AccessKey for a RAM user

Resource Access Management (RAM) is an Alibaba Cloud service that helps you manage user identities and access to your cloud resources. RAM allows you to create and manage multiple identities under an Alibaba Cloud account, and grant diverse permissions to a single identity or a group of identities. In this way, you can authorize different identities to access different Alibaba Cloud resources.

An AccessKey is required when you activate a backup client. If the AccessKey of an Alibaba Cloud account is leaked, all cloud resources under the account may be exposed to risk. Therefore, we recommend that you use the AccessKey of a RAM user to activate backup clients. Before you back up data, make sure that a RAM user is created and an AccessKey is created for the RAM user. For more information, see Create a RAM user and Create an AccessKey pair for a RAM user.

Register a gateway

To register a gateway, perform the following steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > CSG Backup**.
3. In the top navigation bar, select the region where the gateway resides.
4. In the upper-right corner, click **Register Storage Gateway**.
5. In the **Register Storage Gateway** pane, set the parameters. The following table describes the parameters.

Parameter or section	Description
Vault Name	The backup vault where you want to store the backup data. A backup vault is a repository that HBR uses to store backup data. You can use a single vault to store backup data that is received from multiple backup clients. Backup vaults reside in different regions. You can select or create only a backup vault in the current region. ○ If you have created backup vaults, click **Select Vault**, and select a backup vault from the **Vault Name** drop-down list. ○ If you have not created backup vaults, click **Create Vault** and specify the **Vault Name** field. The vault name must be 1 to 64 characters in length.

Parameter or section	Description
Gateway Cluster	The cluster where the gateway resides.
Use HTTPS	Specifies whether to use HTTPS for encrypted data transmission. Note that HTTPS compromises the performance of data transmission. Data that is stored in the backup vault is encrypted, regardless of the setting of this switch. If you modify the setting of this parameter, the modification takes effect on the next migration or restore job.
Gateways	The gateways whose shares you want to back up. Note You can use HBR to back up standard and enhanced CSG file gateways.

6. Click **Create**. HBR then installs a backup client on the ECS instance that hosts each selected gateway.

What to do next

On the **Storage Gateways** tab, you can perform the following operations on a gateway.

Operation	Description
Check the installation status of the backup client	If the backup client is installed, the client status is Activated. If the client status is Installation Failed, it indicates that the installation of a backup client fails. Follow the instructions in the error message to troubleshoot the error. After the error is fixed, choose **More** > **Install Client** in the Actions column.
Uninstall the backup client	Choose **More** > **Uninstall Client** in the Actions column.
Delete the backup client	To uninstall the backup client and remove the gateway, choose **More** > **Remove** in the Actions column. Note Before you delete a backup client, make sure that the client has no running or completed backup jobs.

3.Back up shares of a gateway

You can use Hybrid Backup Recovery (HBR) to back up shares of Cloud Storage Gateway (CSG). You can then restore the shares if they are lost or damaged. This topic describes how to back up shares of a gateway.

Prerequisites

Preparations are completed.

Procedure

1. Log on to the HBR console.
2. Select the region where the gateway resides.
3. In the left-side navigation pane, choose **Backup > CSG Backup**.
4. On the **Storage Gateways** tab, find the gateway, and click **Back Up** in the Actions column.
5. In the **Select Source** step, select the share that you want to back up. Click **Next**.
6. In the **Configure Plan** step, set the parameters and click **OK**. The following table describes the parameters.

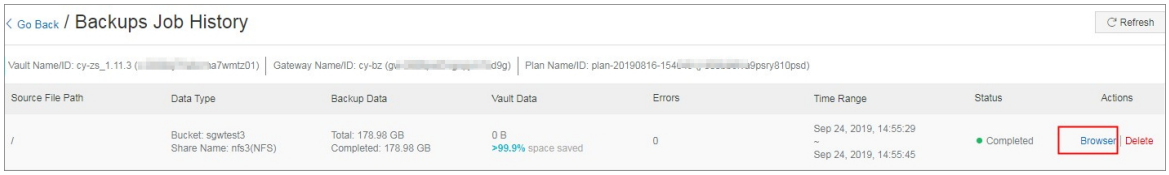
Parameter	Description
Source Paths	○ The paths to the source files. Enter a maximum of eight paths. ○ Each source path must be an absolute path. ○ Uniform Naming Convention (UNC) paths are supported. ○ Separate each path with a carriage return.
Plan Name	The name of the backup plan. By default, a random name is used.
Retention Period	The retention period of the backup data. Unit: days, weeks, months, or years.
Start Time	The start time of the backup plan. The time is accurate to seconds.
Backup Interval	The interval at which data backup is performed. Unit: hours, days, or weeks.
Throttle Bandwidth	Specifies whether to throttle the bandwidth. You can throttle the bandwidth that is used for data backup during peak hours. This guarantees business continuity. If you select **Yes**, you must set the Throttling Period (Hour) and Max Bandwidth parameters. Then, click **Add**.

Query files that are backed up

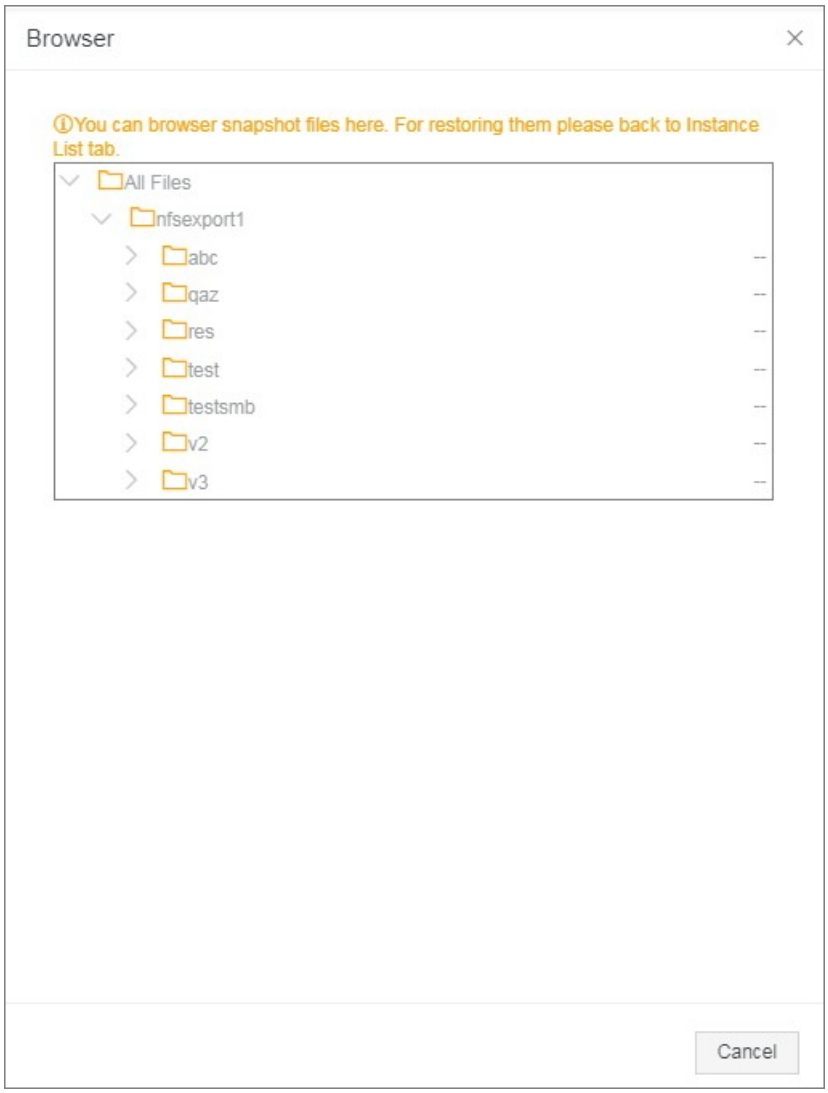
In the HBR console, you can query the list of files that are backed up in each backup plan.

1. On the **Backup Plans and Jobs** tab, find the backup plan, and click **View** in the Actions column.

2. On the page that appears, click **Browser** in the Actions column that corresponds to a source path.



In the **Browse** dialog box, view all files in the source path.



> **Notice** In this dialog box, you can only query the files in the source path but cannot restore the files. For more information, see Restore shares of a gateway.

What to do next

On the **Backup Plans and Jobs** page, you can perform the following operations on a backup plan.

Operation	Procedure
View an error report	Find the backup plan and view the backup progress in the Status column. If the backup of some files fail, click **View** in the Actions column. In the Errors column, click the **Download** icon to download the error report.
Start a backup job	Find the backup plan, and choose **More** > **Run Immediately** in the **Actions** column.
Cancel a running backup job	Find the backup plan, and choose **More** > **Cancel Job** in the **Actions** column.
Pause a running backup job	Find the backup plan, and choose **More** > **Suspend** in the **Actions** column.
Resume a paused backup job	Find the backup plan, and choose **More** > **Resume** in the **Actions** column.
Modify a backup plan	Find the backup plan, and choose **More** > **Modify** in the **Actions** column.
Delete a backup plan	Find the backup plan, and choose **More** > **Delete** in the **Actions** column. **Note** After you delete the backup plan, HBR no longer runs backup jobs for the plan but the backup data is retained.

4.Restore shares of a gateway

You can use Hybrid Backup Recovery (HBR) to restore shares to the source gateway. You can also restore shares to a gateway that resides in the same region as the source gateway.

Procedure

1. Log on to the HBR console.
2. Select the region where the destination gateway resides.
3. In the left-side navigation pane, choose **Backup > CSG Backup**.
4. On the CSG Backup page, click the **Storage Gateways** tab.
5. On the Storage Gateways tab, find the destination gateway, and click **Restore** in the Actions column.
6. In the **Create Restore Job** pane, set the **Restore From** parameter.
   - **Current Gateway**

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

     a. Click **Next**.

     b. Select a backup and click **Next**.

     c. In the **Configure Restore Policy** step, enter a destination path, select a restore policy, specify the files that you want to restore based on the policy, and then click **Create**.
   - **Other Gateway**

     Select this option if you need to restore files from another gateway that uses the same backup vault as the current gateway. Then, perform the following steps:

     a. Select the source gateway and click **Next**.

     b. Select a backup and click **Next**.

     c. In the **Configure Restore Policy** step, enter a destination path, select a restore policy, specify the files that you want to restore based on the policy, and then click **Create**.

What to do next

You can view the status of the restore job on the **Restore Jobs** tab of the **CSG Backup** page. You can also cancel the job when it is running.

5.Configure alert notifications

HBR sends alert notifications to the Alibaba Cloud account owner by default when backup fails or a backup client is disconnected from HBR. You can customize notification contacts, contact groups, and methods.

Create a notification contact

A notification contact is a person who receives backup alerts. To create a notification contact, perform the following steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, click **Notification Contacts**.
3. On the Notification Contacts page, click the **Contacts** tab.
4. In the upper-right corner, click **Create Contact**.
5. In the **Create Contact** dialog box, enter a contact name.
6. Select **Email** as Notification Methods.After you select Email, enter an email address in the **Email** field and click **Send**. Log on to the specified email address and copy the verification code. Then, paste the code in the Verification Code field in the HBR console.
7. Click **OK**.

> Note
>
> - You can view the information of all created notification alerts on the **Contacts** tab.
> - You can click **Modify** to change the email address of a notification contact.
> - You cannot delete a notification contact if the contact is specified to receive alert notifications or added to a contact group.

Create an alarm contact group

If you need multiple alert contacts to receive alert notifications, you can add an alert contact group and add alert contacts to the group so that you can manage them more conveniently. When an alert is generated, HBR sends an alert notification to all alert contacts in the specified alert contact group.

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.

Create alert policies

You can create the following types of alarm policies:

> **Note** By default, HBR sends alert notifications by using emails to the Alibaba Cloud account owner. If you use custom alert policies, a gateway-level alert policy takes precedence over a vault-level alert policy.

- Vault-level alert policy

  A vault-level alert policy applies to all the backup clients that are associated with the vault. The backup clients include those for ECS, on-premises files, and on-premises virtual machines (VMs).

  To configure an alert policy for a vault, perform the following steps:

  i. Log on to the HBR console.
  ii. On the **Overview** page, find the vault.
  iii. In the upper-right corner of the vault card, click the Settings icon.
  iv. In the **Modify Backup Vault** pane, select an alert policy based on your requirements.

Alert policy	Description
Disabled	If you select this option, HBR does not send alert notifications.
Default	If you select this option, HBR sends alert notifications to the Alibaba Cloud account owner by using emails.
Custom	If you select this option, you must select one or more notification contacts or contact groups. HBR sends alert notifications to the selected contacts and contact groups.

  v. Click **OK**.

- Gateway-level alert policy

  A gateway-level alert policy applies to the backup client of a gateway.

  To configure an alert policy for a gateway, perform the following steps:

  i. Log on to the HBR console.
  ii. In the left-side navigation pane, click **CSG Backup**.
  iii. On the **CSG Backup** page, click the **Storage Gateways** tab.
  iv. Find the gateway and choose > **Alert Settings**.

v. In the **Alert Policy** pane, select an alert policy based on your requirements.

Alert policy	Description
Disabled	If you select this option, HBR does not send alert notifications.
Same as Vault	If you select this option, the alert policy of the backup vault where the backup data of the storage gateway is stored applies to the storage gateway.
Default	If you select this option, HBR sends alert notifications to the Alibaba Cloud account owner by using emails.
Custom	If you select this option, you must select one or more notification contacts or contact groups. HBR sends alert notifications to the selected contacts and contact groups.

vi. Click **OK**.

6.Restore shares across regions by using a mirror vault

A backup vault is a repository that Hybrid Backup Recovery (HBR) uses to store backup data on the cloud. A mirror vault is the mirror of a backup vault. The two vaults reside in different regions. You can use a mirror vault for geo-disaster recovery and cross-region data restoration.

Create a mirror vault

To create a mirror vault, perform the following steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, click **Overview**.
3. Find the card of the backup vault for which you want to create a mirror vault. In the upper-right corner of the card, click the

   icon.
4. In the Create Mirror Vault pane, select the region where you want to create the mirror vault.

   > **Note** To implement disaster recovery, do not select the region where the backup vault resides.

5. Enter a vault name. The name must be 1 to 32 characters in length.
6. Enter a description of the vault and click **Create**.

Restore data from a backup stored in a mirror vault

To restore data from a backup that is stored in a mirror vault, perform the following steps:

1. Log on to the HBR console.
2. Select the region where the mirror vault resides. Then, register a storage gateway and set the backup vault to the mirror vault.
3. Restore data to the storage gateway.

   > **Note** In this step, set the Restore From parameter to **Other Gateway**.