Alibaba Cloud

Hybrid Backup

Back up CSG

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

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 manner. You can use the CSG backup service to back up shares of Cloud Storage Gateway (CSG).

CSG is a gateway service that you can deploy in your data center and on Alibaba Cloud. CSG uses Object Storage Service (OSS) buckets as backend storage devices. CSG provides standard file services for on-premises and cloud applications over the Network File System (NFS) and Server Message Block (SMB) protocols. CSG also provides block storage services for on-premises and cloud applications over the Internet Small Computer Systems Interface (iSCSI) protocol. For more information, see What is CSG?.

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

1. Register a gateway

2. Back up shares of a gateway

3. Restore shares of a gateway

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

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

2.Register a gateway

You can use Hybrid Backup Recovery (HBR) to back up shares of Cloud Storage Gateway (CSG). Then, you can restore the shares as needed. Before you back up shares of CSG, you must register a gateway.

Procedure

> ⑦ **Note**   HBR allows you to use the CSG backup service in multiple regions. You can log on to the HBR console to view the regions in which the CSG backup service is supported.

1.
2. In the left-side navigation pane, choose **Backup > CSG Backup**.
3. In the top navigation bar, select a region.
4. On the **Storage Gateways** tab, click **Register Storage Gateway**.
5. In the **Register Storage Gateway** panel, set the parameters described in the following table and click **Create**.

Parameter	Description
Backup Vault	The backup vault where you want to store the backup data. ○ **Create Vault**: Enter a backup vault name to create a backup vault. The vault name must be 1 to 64 characters in length. ○ **Select Vault**: Select a backup vault from the drop-down list. > ⑦ **Note** A backup vault is a repository that HBR uses to store backup data. You can back up data from multiple HBR backup clients to a single vault. Backup vaults reside in different regions. You can select or create a backup vault only in the current region.
Vault Name	The name of the backup vault that stores backup file.
Gateway Cluster	The cluster in which the gateway resides.
Use HTTPS	Specifies whether to use HTTPS to transmit the data that is encrypted and stored in a backup vault. HTTPS is more secure than HTTP in data transmission. If you modify the setting of this switch, the modification takes effect on the next backup or restore job. ○ **No**: HTTPS is not used to transmit data. ○ **Yes**: HTTPS is used to transmit data.
Gateways	In the list of gateways, select the gateway that you want to back up. > ⑦ **Note** You can use HBR to back up only standard and enhanced file gateways.

After you register the gateway, HBR installs a backup client for ECS on the node of the gateway. On the **Storage Gateways** tab, you can view the installation status of the backup client for ECS on the node of the gateway. You can upgrade the HBR client based on your business requirements.

What to do next

On the **Storage Gateways** tab, you can also 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 , the backup client fails to be installed. 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	If you want to uninstall the backup client and delete the gateway, choose **More > Delete** in the Actions column. ⑦ **Note** Before you delete a backup client, make sure that the client has no backup jobs that are running or complete.
Configure the backup client	Specify the maximum number of worker threads, the maximum number of CPU cores, and whether to use HTTPS to transmit data. ● **Use HTTPS**: Specify the protocol over which the client transmits data. ● **Maximum number of worker threads**: Specify the number of threads that work on the client. ● **Maximum CPU Cores**: Specify the maximum number of CPU cores that are used by the client.
View backup records	View the files that are backed up.
Configure alerts	You can choose **More > Alert Settings** in the Action columns and then select a backup alert policy. The following table describes the alert policies. ● **Disabled**: The backup client does not send alert notifications. ● **Same as Vault**: The backup client sends alert notifications in the same way as the backup vault. ● **Default**: The backup client sends alert notifications to the owner of the Alibaba Cloud account by using emails. ● **Customize**: Select one or more contacts or contact groups. Then, the backup client sends alert notifications to the selected contacts or contact groups.

What's next

Back up shares of a gateway

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

A gateway is registered. For more information, see Register a gateway.

Procedure

1.

2.

3.

4. On the **Storage Gateways** tab, find the gateway whose shares you want to back up, and click **Back Up** in the Actions column.

5. In the **Create Backup Plan** panel, select the share that you want to back up and click **Next**.

6. In the **Configure Backup Plan** step of the **Create Backup Plan** panel, set the following parameters and click **OK**.

Parameter	Description
Plan Name	The name of the backup plan. By default, a random name is used.
Source Paths	The paths to the source files, for example, *windows\system* or */us r/local/bin*.
Start Time	The time at which the backup plan starts. The time is accurate to seconds.
Backup Interval	The interval at which incremental backup is performed. Units: hours, days, or weeks.
Retention Policy	**Limited** or **Permanent**. If you select **Limited**, you must select the types of the files that you want to back up from the **Select File Type** drop-down list. If you select **Permanent**, backup files are permanently retained.
Retention Period	This parameter is required only if the Retention Policy parameter is set to **Limited**. Specify the retention period of backup data. Unit: days, weeks, months, or years.

Parameter	Description
Throttle Bandwidth	Specifies whether to throttle the bandwidth. To guarantee business continuity, you can limit the bandwidth that is used for data backup during peak hours. If you turn on Throttle Bandwidth, you must select the Time Range (Hour) based on your business requirements, enter the Max Bandwidth (MB) for backup during the specified time range, and then click **Add**.

What to do next

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

Operation	Description
View	You can query the files that are backed up in each backup plan. Find the backup plan and click **Query** in the **Actions** column to the right of the backup plan.
Run Now	Find the backup plan, and choose **More > Run Now** in the **Actions** column.
Cancel Job	Cancel a backup job that is running. Find the backup plan, and choose **More > Cancel Job** in the **Actions** column.
Suspend	Suspend a backup job that is running. Find the backup plan, and choose **More > Suspend** in the **Actions** column.
Resume	Resume a backup job that is paused. Find the backup plan, and choose **More > Resume** in the **Actions** column.
Modify	Modify a backup plan. Find the backup plan, and choose **More > Modify** in the **Actions** column.
Delete	Delete a backup plan. Find the backup plan, and choose **More > Delete** in the **Actions** column. ⑦ **Note** After you delete a backup plan, HBR no longer runs the plan. However, the backup data is retained.

What's next

Restore shares of a gateway

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.

Prerequisites

The shares of Cloud Storage Gateway (CSG) are backed up. For more information, see Back up shares of a gateway.

Procedure

1.

2.

3.

4. On the **Storage Gateways** tab, find the gateway, and click **Restore** in the Actions column.

5. In the **Create Restore Job** panel, 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 want 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**.

   After you create a restore job, you can view the restoration status of the job on the **Restore Jobs** tab. You can also cancel a restore job that 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.

> 🔊 **Notice**   A contact receives an alert about one hour after backup fails or a backup client is disconnected from HBR.

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**.

   > ⑦ **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 a contact group

You can create a contact group and add multiple notification contacts to the group. Then, you can enable the group to receive the same alert notifications. This simplifies the procedure to manage the notification contacts. When an alert is triggered, HBR sends alert notifications to all contacts in the group.

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 **Groups** tab.

4. In the upper-right corner, click **Create Group**.

5. In the **Create Group** pane, specify a group name.

6. Select the contacts that you want to add to the group and click the ⟩ button. Then, the

selected contacts are added to the Selected Contacts section.

7. Click **OK**.

> ⑦ Note
>> ○ You can view the information of all created contact groups and the number of member contacts in each group on the **Groups** tab.
>> ○ You can click **Modify** to modify a contact group.
>> ○ You cannot delete a contact group if the group is specified to receive alert notifications.

Create alert policies

You can create the following types of alarm policies:

> ⑦ **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 files across regions by using a mirror vault

A backup vault is a cloud warehouse used by Hybrid Backup Recovery (HBR) 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.

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 **Cross-Region Backup**.

4. In the **Create Mirror Vault** panel, set the following parameters and click **Create**.

Parameter	Description
Region	Select the region where you want to create the mirror vault.
Vault Name	The name of the mirror vault. The name must be 1 to 64 characters in length.
Description	The description of the mirror vault.

> ⑦ **Note**   To implement disaster recovery, you cannot select the region where the backup vault resides.

Restore data from a backup stored in a mirror vault

After you create a mirror vault, you can use the mirror vault to restore backup data based on your business requirements. To restore data from a backup file stored in the mirror vault, perform the following steps:

1.

2. In the left-side navigation pane, choose **Backup > CSG Backup**.

3. Select the region where the mirror vault resides and register a gateway for the mirror vault. For more information, see Procedure.

4. Restore data to the gateway. For more information, see Restore shares of a gateway.

> ⑦ **Note**   In this step, set the Restore From parameter to **Other Gateway**.