Alibaba Cloud Hybrid Backup

Back up ECS

Issue: 20190912

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.	 Danger: 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.	 Warning: 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.	 Notice: 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.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

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

Contents

1 Back up files in ECS

1.1 Overview

Hybrid Backup Recovery (HBR) is an efficient, secure, cost-effective, and fully managed backup and storage service. You can use an ECS backup client to back up files from an ECS instance and restore these files when the files are missing or damaged.

This topic includes the following sections:

- Prerequisites
- Start a backup job
- Restore a backup

The following functions are related to this topic:

- Backup alerts
- Mirror vaults

Note:

If you need to back up files from local data centers, see Back up local files.

1.2 Prerequisites

You can use Hybrid Backup Recovery (HBR) to back up files from ECS instances and restore these files as required. The following prerequisites are required before you back up data.

Note:

- To achieve the best backup performance, we recommend that the configurations of a host where a backup client is running meet the following requirements. The host uses a 64-bit CPU with more than two cores and more than 8 GB available memory.
- The size of data that a host can back up is determined by available memory resources. For a host with 4 GB of available memory, the maximum number of

files that you can back up on the host is one million and the total size of data is 8 TB.

- You can only use HBR to back up data from ECS instances that are located in one of the following regions: China (Hangzhou), China (Shanghai), China (Beijing), and China (Shenzhen).

Authorize roles

When using Hybrid Backup Recovery (HBR) to back up files from ECS instances, you must authorize two roles: AliyunHBRDefaultRole and AliyunECSAccessingHBRRole. After the authorization, HBR and ECS are accessible by each other. Proceed as follows:

1. Log on to the HBR console.
2. Choose ECS Backup > ECS File Backup.
3. Authorization pages appear one by one, which require you to confirm the authorization of these roles.

Cloud Assistant

- An ECS backup client must work with Cloud Assistant. By default, Cloud Assistant clients are installed on ECS instances that are created after Dec 1, 2017. When ECS instances from which you need to back up data are purchased before Dec 1, 2017, you must manually install a Cloud Assistant client.
- When ECS instances that are located in a classic network have Cloud Assistant clients installed, you need to use the following steps to configure a Cloud Assistant client.
  - For an ECS instance running Windows
    1. Connect to the ECS instance. In the `C:\ProgramData\aliyun\assist\` folder, create a file named `region-id` and enter the value of the corresponding `region-id` parameter based on the region where the

ECS instance is located. For example, for an ECS instance that is located in the China (Hangzhou) region, you need to enter `cn - hangzhou`.

```
echo   cn - hangzhou  > C :\ ProgramDat  a \ aliyun \ assist \
region - id
```

Regions and corresponding region-ids are listed in the following table.

Region	region-id
China (Hangzhou)	cn-hangzhou
China (Shanghai)	cn-shanghai
China (Beijing)	cn-beijing
China (Shenzhen)	cn-shenzhen

2. Restart the AliyunService service by using Task Manager.

- For an ECS instance running Linux

1. Connect to the ECS instance. In the */ usr / local / share / aliyun - assist /* folder, create a file named `region - id` and enter value the corresponding `region  id` parameter based on the region where the ECS instance is located. For example, for an ECS instance that is located in the China (Hangzhou) region, you need to enter `cn - hangzhou`.

```
echo   cn - hangzhou  >/ usr / local / share / aliyun - assist
/ region - id
```

Regions and corresponding region IDs are listed in the following table.

Region	region-id
China (Hangzhou)	cn-hangzhou
China (Shanghai)	cn-shanghai
China (Beijing)	cn-beijing
China (Shenzhen)	cn-shenzhen

2. Run the `chkconfig  agentwatch  off` command and the `chkconfig  agentwatch  on` command. Alternatively, you can run the `systemctl  restart  agentwatch` command to restart the Cloud Assistant client.

Note:

If the issue persists after you restart the Cloud Assistant client, you need to restart the Cloud Assistant client by using the preceding commands.

Install an ECS backup client

You can use an ECS backup client to back up files from an ECS instance and restore these files. You can use one of the following methods to install ECS backup clients.

- Install ECS backup clients by selecting ECS instances: installs backup clients for selected ECS instances.
- Install ECS backup clients by using a template: installs backup clients for ECS instances by using a template.

Install ECS backup clients by selecting ECS instances

Proceed as follows:

1. Log on to the HBR console.
2. Select a region where ECS instances that you need to back up are located.
3. In the left-side navigation pane, choose ECS Backup > ECS File Backup.
4. In the upper-right corner, click Add ECS Instance.
5. In the Add ECS Instance dialog box, enter the Backup Vault Name. On the drop-down list, select an existing backup vault. If no backup vault exists, click Create Vault, and enter the Vault Name and Vault Description to create a new vault. A vault name must be less than 64 characters in length.

    Note:
   Backup vaults are HBR cloud storage repositories that you can use to store backups. You can back up data from multiple ECS instances to the same vault. Backup vaults are located in different regions. You can only select or create backup vaults in the current region.
6. Select one or more ECS instances on which you need to install a backup client. On the left side of `Search`, you can also select `Instance ID`, `Instance Name`, `VPC ID`, `Private IP (VPC)`, and `Internal IP (Classic)`. Then, enter a full name or keyword to search for one or more instances.

    Note:

   - You can only select or search for ECS instances that are located in the current region.

- If you select ECS instances that are located in a `classic network`, you must enter the AccessKey ID and AccessKey Secret.

7. After the configurations are complete, click Create and then backup clients will be installed on the selected ECS instances.

Install ECS backup clients from a template

Proceed as follows:

1. Log on to the HBR console.
2. Select a region where ECS instances that you need to back up are located.

Note:
After selecting a region, you can only install multiple backup clients for ECS instances that are located in the region.

3. In the left-side navigation pane, choose ECS Backup > ECS File Backup.
4. In the upper-left corner of the page, choose Batch Operation > Batch Add ECS Instances.
5. In the Batch Add ECS Instance dialog box, enter the Backup Vault Name to create a new backup vault, and then enter the Vault Description. The vault name must be less than 64 characters in length.

Note:
Backup vaults are located in different regions. You can only select or create backup vaults in the current region.

6. (Optional) You can specify the `Private IP (VPC)` or `Internal IP (Classic)` of ECS instances on which you need to install backup clients.

Note:

- After you specify one or more IP addresses, only ECS instances that correspond to the IP addresses are displayed in a template.
- If no IP address is specified, all ECS instances that are located in the current region are displayed in a template.
- Separate multiple IP addresses with commas (,).

7. Click Download Template.

8. Open the template, enter the AccessKey ID and AccessKey Secret, and then save the template. You do not need to enter the AccessKey ID or AccessKey Secret for an ECS instance when the network type is VPC.

   Note:

   - Only ECS instances that have Cloud Assistant clients and backup clients installed are displayed in a template.
   - If you add more than 20 ECS instances at a time, new vaults are created to host additional ECS instances.
   - If you do not need to install a backup client on an ECS instance, you can delete the row where the ECS instance is located.
   - We recommend that you do not change the column headers, such as Instance ID, Instance Name, and Network Type.
   - We recommend that you delete the local template after uploading the template to ensure account security.

9. Click Upload Template to upload the template.

After a template is uploaded, the number of each type of specified ECS instances and the total number of ECS instances are displayed in the Batch Add ECS instance dialog box.

Manage backup clients

On the ECS File Backup page, select ECS Instance tab and locate the target ECS instance. For a large number of ECS instances, in the `Search` field that is located in the upper-right corner of the page, enter the `Private IP (VPC)` or `Internal IP (Classic)` to search for the target instance.

After locating the target ECS instance, you can perform the following actions.

Action	Description
View the installation status of a backup client	If a client installation is successful, the status is displayed as `Activated`. If the status is `Failed`, follow instructions provided in the error message, click the More icon next to the ECS instance, and select Re-install.
Uninstall a client	In the Actions column, choose More > Uninstall Client.

Action	Description
Delete a client	If you need to delete an ECS instance from a list of ECS instances and uninstall the backup client from the ECS instance, choose More > Delete next to the instance. Note: You must ensure that no running or completed backup job exists on a backup client before deleting this client.
Update a backup client	Locate the target ECS instance, click Update to update the client to the latest version.

Subsequent operations

Back up files from an ECS instance

1.3 Back up files from an ECS instance

You can use Hybrid Backup Recovery (HBR) to back up files that are located on an ECS instance. When files are missing or damaged, you can restore these files by using a backup. This topic describes how to back up files that are located on an ECS instance.

Note:
You can only back up files from an ECS instance that is located in one of the following regions: China (Hangzhou), China (Shanghai), China (Beijing), and China (Shenzhen).

Prerequisites

You have completed the preparation.

Back up files from a single ECS instance

You can use HBR to back up files from a single ECS instance. Proceed as follows:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose ECS Backup > ECS File Backup.
3. On the ECS File Backup page, select the ECS Instance tab.
4. Locate the target ECS instance, and click Backup in the Actions of the instance.

5. In the Create Backup Plan dialog box, configure the required settings based on the following descriptions, and click Create.

Name	Description
Source Path	· The path of a 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. · A source path must be an absolute path. · You can enter a Uniform Naming Convention (UNC) path as a source path. Note: When the source path is a UNC path, Windows access control lists (ACLs) are not backed up. · Separate source paths with carriage returns.
Plan Name	The name of the plan. If you leave this field blank, a random name is specified by default.
Retention	The retention period of a backup. Unit: day, week, month, and year.
Start Time	The start time of the plan. The time is accurate to the second .
Plan Interval	Specify the frequency of incremental backups. Unit: day, week, month, and year.
Delete Source Files	If you need to delete source files after a backup is complete, select Delete.
Use VSS for backup	· The feature is only available for instances running Windows. · If you need to ensure data consistency between a backup source and its backup when data changes occur in the backup source, you can select Use. · If you use Volume Shadow Copy (VSS), you cannot back up data from multiple directories at a time. Note: You cannot use VSS for backup when the backup source is on an exFAT volume.

Name	Description
Using Flow Control	You can use flow control to set bandwidth limits for backing up data from a directory during peak hours. This ensures business continuity. If you select Use, you need to select a `Time Range` based on business requirements. Enter the maximum allowed bandwidth during the specified time range in the `Max Flow` field, and click Add.

Back up files from multiple ECS instances

If you need to back up files from multiple ECS instances, you can create multiple backup plans at a time. Proceed as follows:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose ECS Backup > ECS File Backup.
3. At the top of the page, select the region of the ECS instance from which you need to back up data.
4. In the upper-right corner, choose Batch Operation > Batch Add Backup Plan.
5. In the Batch Add Backup Plan dialog box, click Download Template.
6. Open the downloaded template, follow instructions to configure the template, and save the template.

> Note:
> If you do not need to back up an ECS instance, you can delete the row where the instance is located.

Name	Description
Client ID	The ID of the available client you can use to back up data. We recommend that you do not change the ID.
Instance ID	The ID of the ECS instance where the client is located. We recommend that you do not change the ID.
Instance Name	The name of the ECS instances where the client is located. We recommend that you do not change the name.

Name	Description
Source	The path of a directory from which you need to back up data. A path must be an absolute path.
Plan Name	The name of a plan. If you leave this field blank, a random name is specified by default.
Retention Day	· The retention period of a backup . You must enter an integer as the value. · Unit: day (by default). · If you leave this empty, the backup file is saved for 730 days by default.
Effective Time	The start time of a backup. The format is `YYYY - MM - DD / HH : MM : SS` . For example, 2018-12-03/12:00:00.
Backup Interval	· Enter an interval between two incremental backups. You must enter an integer as the value. · Unit: hour (by default). · If you leave this field blank, the interval is 24 hours by default.
Use VSS for backup	· This feature is only available for instances running Windows. · You can enable this feature when data changes occur in the backup source. The feature is designed to help ensure data consistency between a backup source and a backup. · Enter `Y` to enable this feature and enter `N` to disable this feature. If you leave this field blank, the feature is disabled by default. · If you use VSS, you cannot back up multiple directories at a time.

Name	Description
Bandwidth Throttling	· Flow control. You can set bandwidth limits for backing up directories to ensure business continuity. · If you enable this function, enter the maximum bandwidth that can be consumed by a backup job during a specified time range. · You must enter an integer as the value. Unit: MB (by default). · If you leave this field blank, the bandwidth is not throttled.

7. Click Upload Template to upload the template.
8. Click Create.

More actions

On the ECS File Backup page, select the Backup Plan and Job tab. You can perform the following actions.

Action	Procedure
View an error report	In the Actions column, you can click View to show the progress of a backup plan. If a number of files failed to back up, you can click View next to a backup plan. Click the Download icon next to the `number of failed files` to download the Error Report.
Run a backup job	In the Actions column, click the More icon next to a backup plan and select Execute Now.
Cancel a running backup job	In the Actions column, click the More icon next to a backup plan and select Cancel Task.
Pause a running backup job	In the Actions column, click the More icon next to a backup plan and select Pause.
Resume a running backup job	In the Actions column, click the More icon next to a backup plan and click Enable.
Modify a backup plan	In the Actions column, click the More icon next to a backup plan and select Edit.
Delete a backup plan	In the Actions column, click the More icon next to a backup plan and select Delete. After you delete a backup plan, the backup plan is no longer running. However, data that you have already backed up by using the plan is retained.

1.4 Restore data from a backup to an ECS instance

You can restore files to an ECS instance from a backup stored on it or another ECS instance in the same vault. You can also restore files to an ECS instance from a backup that is created by a backup client.

Procedure

1. Log on to the Hybrid Backup Recovery (HBR) console.
2. In the left-side navigation pane, choose ECS Backup > ECS File Backup.
3. On the ECS File Backup page, select the ECS instance tab.
4. Locate the target ECS instance, and click Restore in the Actions column of the instance.

5. In the New Restore Task dialog box, select a `Restore Source`.
   - From this ECS

     If you need to restore data from a backup stored on this ECS instance, you can select this option and perform the following steps.

     a. Click Next.
     b. Select a snapshot, and click Next.
     c. Enter the `Restore Path`, select files to be restored, and click Create.
   - From Other ECS

     If you need to restore data from a backup stored on another ECS instance in the same vault to this ECS instance, you can select this option and perform the following steps.

     a. Select an ECS instance where the backup is located and click Next.
     b. Select a snapshot and click Next.
     c. Enter the `Restore Path`, select files to be restored, and click Create.
   - From Local Client

     If you need to restore a backup that is created by a file client from a local data center to this ECS instance, you can select this option and perform the following steps.

     a. Select a local host where the required backup is located and click Next.
     b. Select a snapshot, and click Next.
     c. Enter the `Restore Path`, select files to be restored, and click Create.

 Note:
On the ECS File Backup page, select the Restore Jobs tab to view the progress of the new restore job.

1.5 Backup alerts

Backup alerts provide you with alerts, such as when a backup fails or a client is disconnected from a server. By default, alerts are sent to an Alibaba Cloud account. You can also configure contacts, contact groups, and contact methods.

 Note:

One hour after a backup fails or a client is disconnected from a server, the specified contact will receive an alert.

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 Verificati on` field.
   - Mobile

     If you select Mobile as a contact method, enter the Mobile and then clickSend Verification. An SMS message that contains a verification code will be sent to your mobile phone. Enter the verification code in the `Mobile Verificati on 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 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.

Customize alert policies

You can customize the following types of alert policies:

> Note:
> By default, HBR sends alert notifications by SMS or email to the alert contact specified in your Alibaba Cloud account. If you customize alert policies, the instance-level alert policy takes precedence over the vault-level alert policy.

- Vault-level alert policy

  A vault-level alert policy applies to all the backup clients of a vault. The backup clients include those installed on Alibaba Cloud Elastic Compute Service (ECS) instances, local hosts, and local virtual machines.

  Set a vault-level alert policy as follows:

  1. Log on to the HBR console.
  2. On the Overview page, find the vault for which you need to set an alert policy.
  3. In the upper-right corner of a vault card, click the Settings icon.
  4. In the Vault Setting dialog box, set `Alarm Policy` as required.
     - Disabled

       If you select this option, HBR does not send an alert notification when an alert is generated for a backup client or an instance that is related to the vault.
     - Default Notification

       If you select this option, HBR sends alert notifications by SMS or email to the alert contact specified in your Alibaba Cloud account when backup alerts are generated for the vault.
     - Customized Notification

       If you select this option, you can specify one or more alert contacts or alert contact groups. Then, HBR sends alert notifications to the specified alert contacts or alert contact groups when backup alerts are generated for the vault.
  5. Click OK.

- Instance-level alert policy

  An instance-level alert policy applies to all ECS backup clients of an SAP HANA instance.

  Set an instance-level alert policy as follows:

  1. Log on to the HBR console.
  2. Find the SAP HANA instance for which you need to set an alert policy. In the right-side Actions column, click Alarm Setting for the instance.
  3. In the Alarm Policy dialog box, set `Alarm Policy` as required.

Alarm policy	Description
`Disabled`	If you select this option, HBR does not send an alert notification when an alert is generated for the SAP HANA instance.
`Same as Vault`	If you select this option, the alert policy of the vault where the SAP HANA instance is located applies to the instance.
`Default Notificati on`	If you select this option, HBR sends alert notifications by SMS or email to the alert contact specified in your Alibaba Cloud account when backup alerts are generated for the SAP HANA instance.
`Customized Notificati on`	If you select this option, you can specify one or more alert contacts or alert contact groups. Then, HBR sends alert notifications to the specified alert contacts or alert contact groups when backup alerts are generated for the SAP HANA instance.

  4. Click OK.

1.6 Mirror vaults

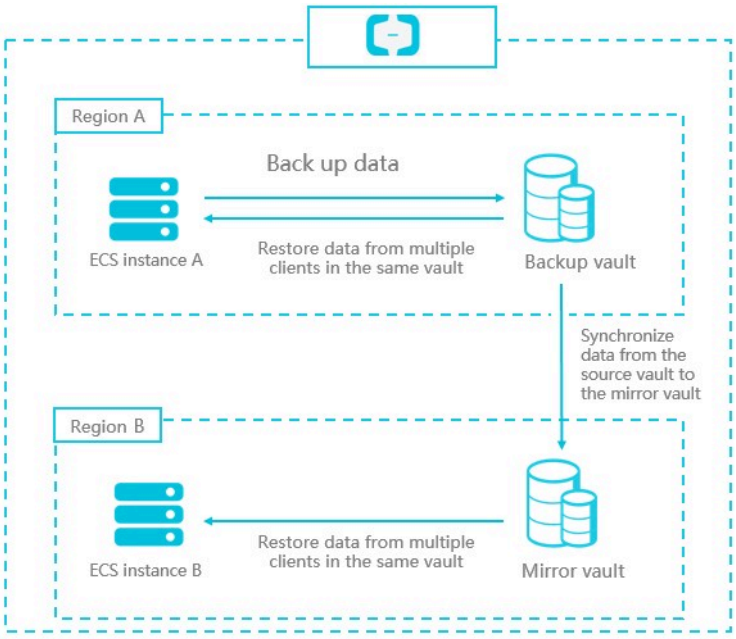
A backup vault is a Hybrid Backup Recovery (HBR) warehouse used to store backup data on the cloud. You can create a remote mirror vault for a backup vault to meet disaster recovery requirements. You can also use a mirror vault for geo-disaster recovery or cross-region data restoration.

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 Descriptio n` as required, and click Create.

Restore data from a backup stored in a mirror vault

If you attempt to restore data from a backup stored in a remote mirror vault, log on to the Hybrid Backup Recovery (HBR) console on an ECS instance that is located in the target region. Proceed as follows:

1. Install a backup client on an ECS instance.

   > Note:
   > Select the target mirror vault when selecting a vault.

2. Locate the ECS instance in the HBR console, and then use the ECS instance to restore data from a backup.

   > Note:
   > In the Restore Source field, select From Other ECS or From Local Client as required.

2 Back up SAP HANA databases in ECS

2.1 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 an Alibaba Cloud Elastic Compute Service (ECS) backup client for HBR to back up SAP HANA databases deployed on ECS instances and restore these databases as required.

For more information about how to back up SAP HANA databases, see the following topics:

- Preparations
- Back up an SAP HANA database
- Restore an SAP HANA database

For more information about other features of SAP HANA database backup, see the following topics:

- Set a log backup policy
- Configure a backup profile
- Configure the backup alerting feature

 Note:
For more information about how to back up SAP HANA databases deployed in a local IDC, see Workflow-based backup.

2.2 Preparations

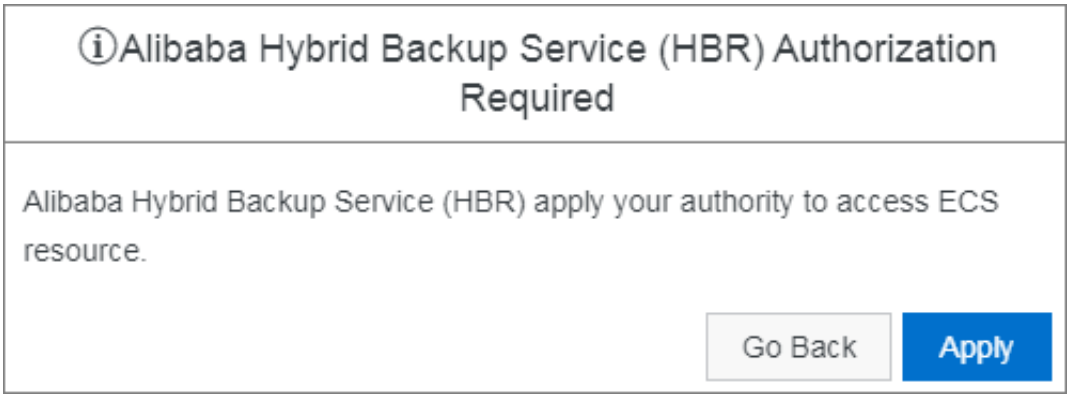
You can use Hybrid Backup Recovery (HBR) to back up SAP HANA databases deployed on Alibaba Cloud Elastic Compute Service (ECS) instances and restore these databases

as required. This topic describes the preparations that you need to make before backing up data.

Authorize roles

Before using HBR to back up files from ECS instances, you must authorize two roles AliyunHBRDefaultRole and AliyunECSAccessingHBRRole to access your cloud resources. The procedure is as follows:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose ECS Backup > ECS File Backup. Authorization dialog boxes appear one by one. Follow instructions to authorize the two roles to access your cloud resources.



Install Cloud Assistant

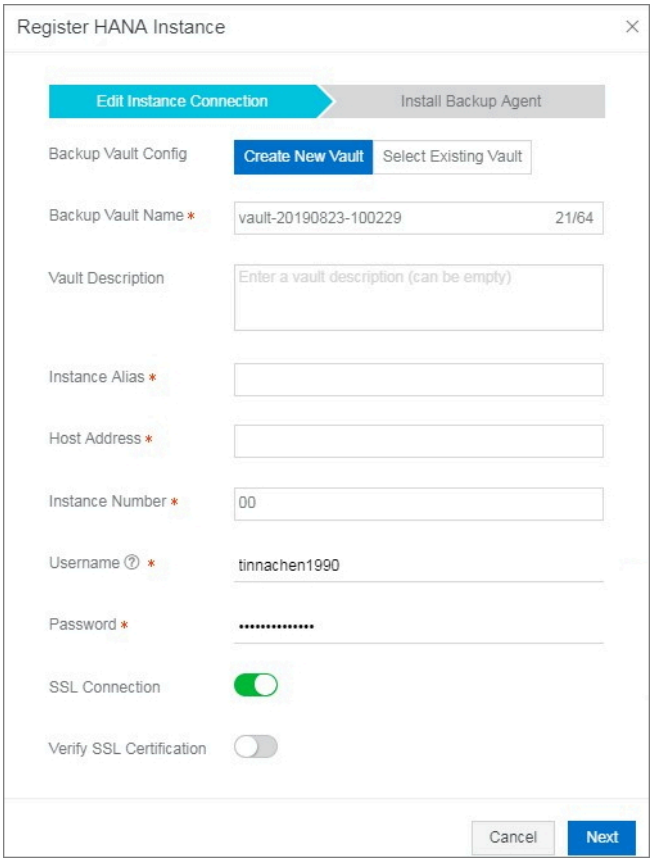
An ECS backup client must work with Cloud Assistant. By default, a Cloud Assistant client is installed on ECS instances that are created after December 1, 2017. To back up files from ECS instances that you bought before December 1, 2017, you must install a Cloud Assistant client.

Register an SAP HANA instance

When you register an SAP HANA instance, you need to configure the connection information about the SAP HANA instance. After the SAP HANA instance is registered , an ECS backup client is installed on each node of the SAP HANA instance. The procedure is as follows:

1. Log on to the HBR console.
2. Select a region where ECS instances that you need to back up are located.
3. In the left-side navigation pane, choose ECS Backup > SAP HANA Backup.
4. In the upper-right corner, click Register HANA Instance.

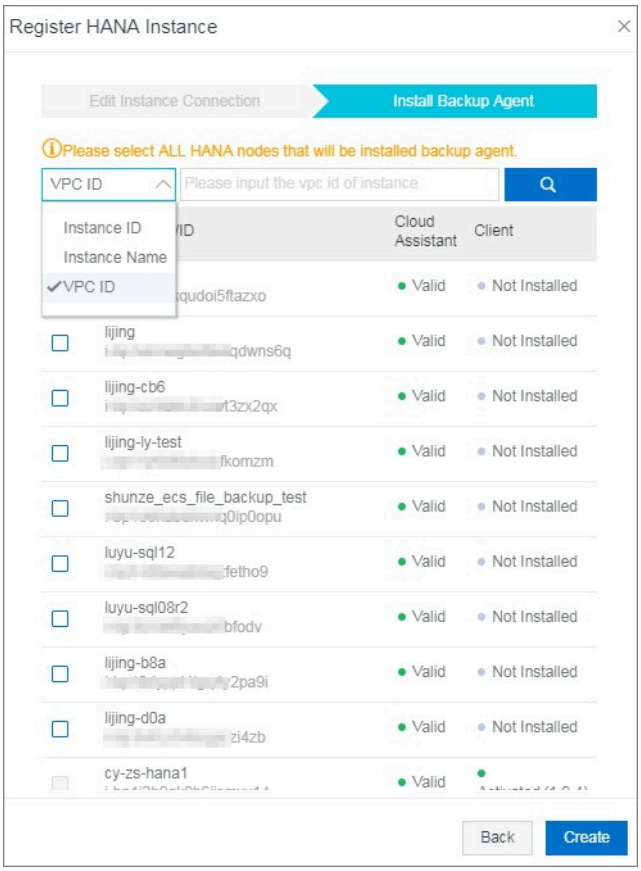
5. In the Register HANA Instance dialog box, set the parameters as instructed in the following table.



Parameter	Description
Backup Vault Name	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. · If you have created backup vaults: Click Select Existing Vault and select a vault from the drop-down list. · If you have not created any backup vaults: Click Create New Vault, and then set Backup Vault Name and Vault Description to create a vault. The vault name cannot exceed 64 bytes in length.
Instance Alias	Enter an alias for the SAP HANA instance to be backed up.
Host Address	Enter the IP address of the SAP HANA primary node.
Instance Number	Enter the instance number that is specified when you install SAP HANA.

Parameter	Description
Username	Enter the username used to log on to the SAP HANA instance.
Password	Enter the password used to log on to the SAP HANA instance.
SSL Connection	Specify whether to use Secure Sockets Layer (SSL) to connect to SAP HANA databases.
Verify SSL Certification	Specify whether to verify SSL certification for the database server if you enable the SSL connection.

6. Click Next.
7. Select all nodes of the SAP HANA instance to be registered, so that HBR can install an ECS backup client on these nodes. In the drop-down list on the left of the search box, select Instance ID, Instance Name, or VPC ID as the keyword. Enter a complete or partial ID or name in the search box to search for ECS instances.



8. After the configuration is completed, click Create. HBR automatically installs an ECS backup client on the selected ECS instances.

Note:

After the SAP HANA instance is registered, you can click the SAP HANA Instance tab on the SAP HANA Backup page. On this tab, you can view the registration

information and status of the registered SAP HANA instance. In the right-side Actions column, you can choose More > Edit Instance to modify the SAP HANA instance.

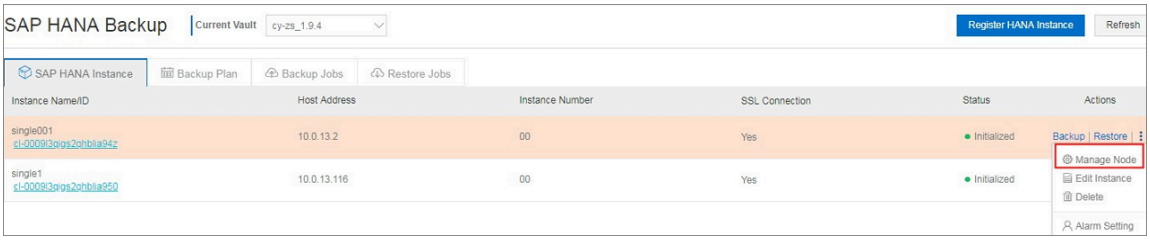
View and manage nodes

After the SAP HANA instance is registered, you can view the installation status of the ECS backup client on each node of the SAP HANA instance. Ensure that an ECS backup client is installed on all nodes to be backed up. You can also enable the node verification feature to install an ECS backup client on newly added nodes.

- Check the client installation status

  To check the installation status of the ECS backup client on a node, perform the following operations:

  1. Ensure that the SAP HANA instance is registered. On the SAP HANA Backup page, click the SAP HANA Instance tab.
  2. In the `Actions` column, choose More > Manage Node for the target SAP HANA instance.



  3. Click the Node Info tab to view the installation status of the ECS backup client on nodes. If the ECS backup client is installed, the node status is Activated. In this case, you can also perform the following operations:

     - Upgrade a backup client

       To upgrade the backup client on a node, click Upgrade in the `Client Type` column for the node.

       Note:

During the upgrade, you need to disable the SAP HANA database backup feature. For more information, see SAP Note 2009486.

- Reinstall a backup client

  If the backup client fails to be installed on a node, choose More > Re-install in the right-side Actions column for the node.

- Uninstall a backup client

  To uninstall the backup client from a node, choose More > Uninstall Client in the right-side Actions column for the node.

- Delete a backup client

  To uninstall the backup client from a node and delete the node, click Delete in the right-side Actions column for the node.

  Note:
  Before deleting a backup client, you need to ensure that the backup client has no backup job in the Running or Completed state.

- Verify nodes

  When you enable the node verification feature, HBR automatically detects changed nodes in the SAP HANA cluster and ECS instances that no longer belong to the cluster. If a node is added to the cluster, HBR reminds you to install an ECS backup client for the node. If HBR detects an ECS instance that does not belong to the SAP HANA cluster, HBR reminds you to uninstall the ECS backup client from the instance. The procedure is as follows:

  1. Ensure that the SAP HANA instance is registered. On the SAP HANA Backup page, click the SAP HANA Instance tab.
  2. In the `Actions` column, choose More > Manage Node for the target SAP HANA instance.
  3. In the upper-right corner of the HANA Instance Info page, click Verify HANA Node.
  4. In the Verify HANA Node dialog box, check node information.
  5. Select nodes for which you need to install or uninstall the ECS backup client.
  6. Click Confirm & Execute.

Note:

You can also perform the following operations:

- Add a node

  On the HANA Instance Info page, click Add HANA Node, select the ECS instance on which you need to install an ECS backup client, and then add this ECS instance as a node to the SAP HANA cluster.
- View databases on an SAP HANA instance

  On the HANA Instance Info page, click the Database tab. On this tab, you can view the status of all databases on the SAP HANA instance.

Configure database backup

To improve the performance of SAP HANA database backup, we recommend that you use Backint and set a log backup policy. For more information, see Configure a backup profile and Set a log backup policy.

Note:
You can also enable the backup alerting feature. This feature enables HBR to send your alert contact an alert notification if a backup fails or a client is disconnected from a server.

2.3 Back up an SAP HANA database

You can use Hybrid Backup Recovery (HBR) to back up SAP HANA databases deployed on Alibaba Cloud Elastic Compute Service (ECS) instances and restore these databases as required. This topic describes how to back up an SAP HANA database.

Prerequisites

Preparations are completed.

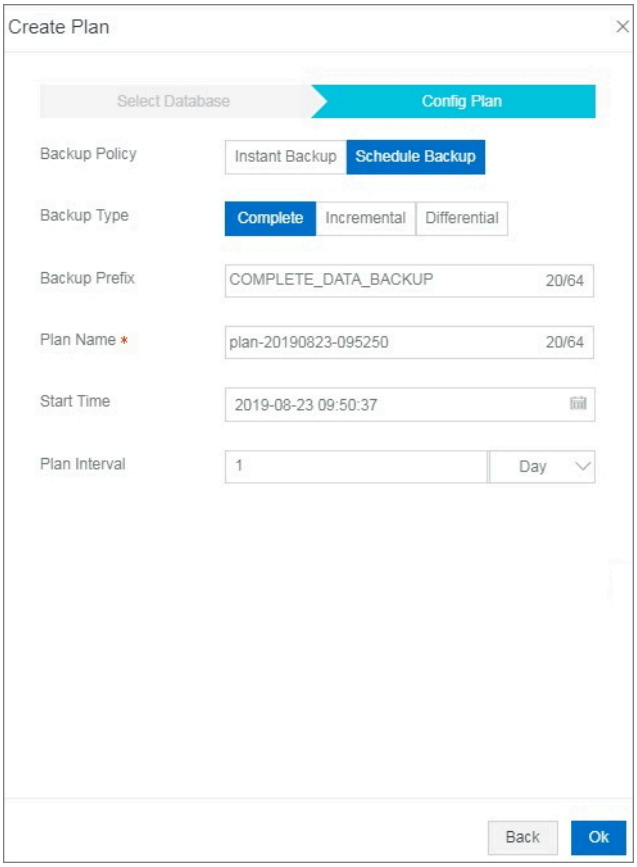
Procedure

1. Log on to the HBR console.
2. In the left-side navigation pane, choose ECS Backup > SAP HANA Backup.
3. Click the SAP HANA Instance tab.
4. In the right-side Actions column, click Backup for the SAP HANA instance to be backed up.

5. In the Create Plan dialog box, select the database to be backed up, and then click Next.

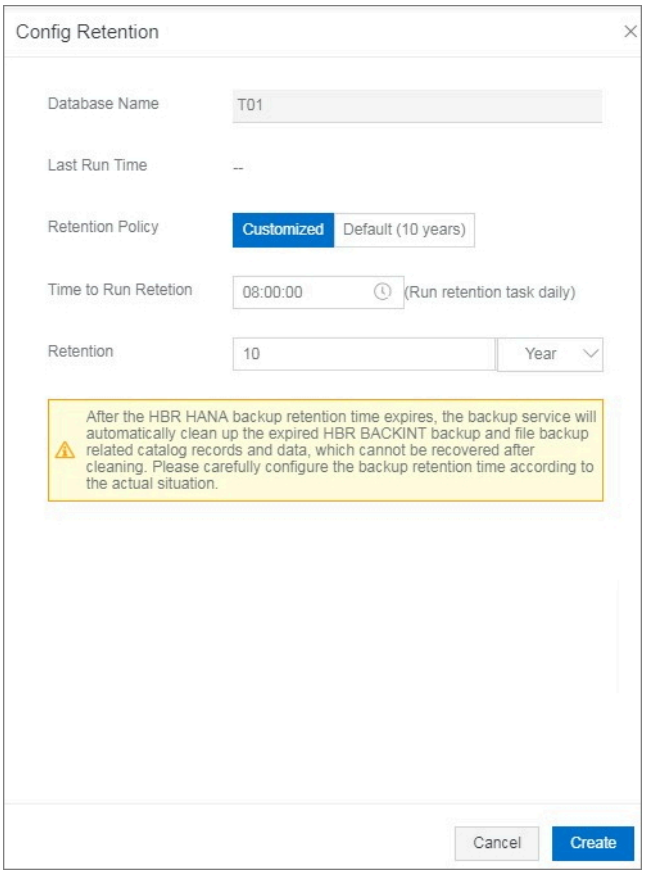
> **Note:**
> You cannot back up databases that are stopped.

6. Set `Backup Policy`. If you do not need to regularly back up the database, select Instant Backup. Otherwise, select Schedule Backup.



7. Set Backup Type. Backup types are described as follows:
   - Complete: backs up full data in the database.
   - Differential: backs up data modified after the last full backup.
   - Incremental: backs up data modified after the last full backup, incremental backup, or differential backup.
8. Set Backup Prefix.
9. If you select Schedule Backup, you also need to set Plan Name, Start Time, and Plan Interval.
10. Click OK.

11. By default, HBR keeps SAP HANA database backup data for 10 years. To customize the retention period, perform the following operations:
    a. On the SAP HANA Backup page, click the `SAP HANA Instance` tab.
    b. Click the instance name or choose More > Manage Node in the right-side `Actions` column for the target SAP HANA instance. The HANA Instance Info page appears.
    c. On the HANA Instance Info page, click the Database tab, find the target database, and then choose More > Config Retention in the right-side Actions column.
    d. In the Config Retention dialog box, set the parameters as instructed in the following table.



Parameter	Description
Retention Policy	· Default (10 years) Select this option if you want to keep backup data for 10 years. HBR automatically deletes the backup data when the retention period expires. · Customized By selecting this option, you can customize the time for deleting expired backup data each day and the backup retention period.
Time to Run Retention	Specify the time for deleting expired backup data. The time is accurate to seconds. We recommend that you specify a time other than business and backup peak hours.
Retention	Specify the retention period of backup data. Valid units: day, week, month, and year. Maximum retention period: 10 years. Note: After the retention period expires, HBR automatically deletes the expired catalogs and data related to Backint backup and file backup. This operation is unrecoverable. Specify the retention period with caution.

e. Click Create.

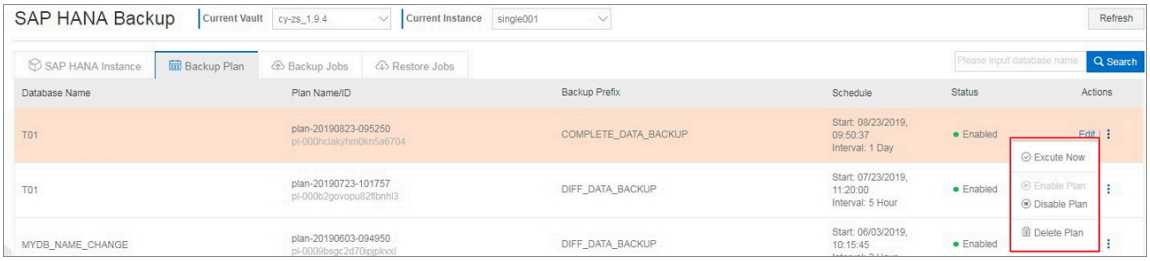
Note:
To modify the backup retention period, you can repeat the preceding steps and specify another retention period.

Related operations

- Manage a backup plan

  In the HBR console, you can view the information and status of created backup plans, and manage these backup plans. The procedure is as follows:

  1. Log on to the HBR console.
  2. In the left-side navigation pane, choose ECS Backup > SAP HANA Backup.
  3. Click the Backup Plan tab.
  4. Check the backup plan information and status on the Backup Plan tab.
  5. Click an operation in the Actions column to manage a backup plan. Operations in the Actions column are Edit, Excute Now, Disable Plan, Enable Plan, and Delete Plan. After you delete a backup plan, HBR does not run the plan any more but reserves backup data.



- View and cancel a backup job

  You can view the status of Instant Backup jobs and Schedule Backup jobs. You can also cancel an ongoing backup job. The procedure is as follows:

  1. Log on to the HBR console.
  2. In the left-side navigation pane, choose ECS Backup > SAP HANA Backup.
  3. Click the Backup Jobs tab.
  4. Check the backup job information and status on the Backup Jobs tab.
  5. To cancel an ongoing backup job, click Cancel in the right-side Actions column for the job.

- View backup history

  You can view all backup history in the HBR console. The procedure is as follows:

  1. Log on to the HBR console.
  2. In the left-side navigation pane, choose ECS Backup > SAP HANA Backup.
  3. Click the SAP HANA Instance tab.
  4. In the right-side Actions column, choose More > Manage Node for the target SAP HANA instance.
  5. On the HANA Instance Info page, click the Backup History tab.
  6. View backup job details on the Backup History tab.

2.4 Restore an SAP HANA database

After using Hybrid Backup Recovery (HBR) to back up SAP HANA databases to a backup vault, you can restore the SAP HANA databases to the original SAP HANA instance or another SAP HANA instance that uses the same backup vault.

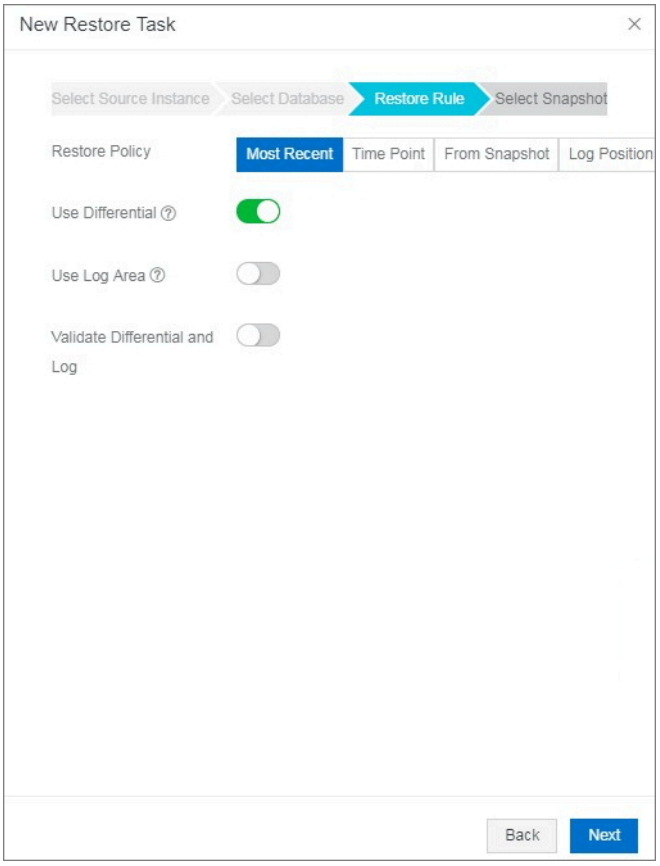
Note:
When restoring SAP HANA databases, HBR automatically stops these databases. As a result, you cannot access these databases during restoration.

Procedure

1. Log on to the HBR console.
2. In the left-side navigation pane, choose ECS Backup > SAP HANA Backup.
3. Click the SAP HANA Instance tab.
4. Find the SAP HANA instance to be restored, and click Restore in the `Actions` column.
5. In the New Restore Task dialog box, select the source SAP HANA instance and click Next.
6. Verify the information about the source SAP HANA instance and the destination SAP HANA instance. Set Source System Name, select a database on the destination SAP HANA instance, and then click Next.

Note:
The Source System Name parameter specifies the name of the source database. Enter the name in the following format: `Source database name @ SID`.

7. **Set Restore Policy and other parameters as required. The following table describes restoration policies.**



Restoration policy	Description	Parameter
Most Recent	Restores the database to the latest available status.	· Use Differential: Turn on this switch if you want to use differential backup or incremental backup to restore the database. If you turn off this switch, HBR uses log backup to restore the database. · Use Log Area: specifies whether to initialize a log area. If you turn on this switch, you initialize the log area and cannot use log entries in this log area. Set this parameter as required. You can turn on this switch when the log area is unavailable, or you want to restore the database to a different system. · Validate Differential and Log: If you turn on this switch, HBR checks the availability of the required differential backup and log backup when the restoration job starts. If the differential backup or the log backup is unavailable, HBR stops the restoration job until the backup data is available.

Restoration policy	Description	Parameter
`Time Point`	Restores the database to the status at a specified time point.	· Use Differential: Turn on this switch if you want to use differential backup or incremental backup to restore the database. If you turn off this switch, HBR uses log backup to restore the database. · Use Log Area: specifies whether to initialize a log area. If you turn on this switch, you initialize the log area and cannot use log entries in this log area. Set this parameter as required. You can turn on this switch when the log area is unavailable, or you want to restore the database to a different system. · Validate Differential and Log: If you turn on this switch, HBR checks the availability of the required differential backup and log backup when the restoration job starts. If the differential backup or the log backup is unavailable, HBR stops the restoration job until the backup data is available. · Restore to Time: Select a time point that you want to restore the database to. HBR restores the database to the status closest to the specified time point.
`From Snapshot`	Restores the database to a specified backup.	· Use Catalog: specifies whether to restore the database from catalog backup. · Backup Prefix: If you turn off Catalog, you need to specify the prefix of a backup file. This allows HBR to find the backup file to restore the database.

Restoration policy	Description	Parameter
`Log Position`	Restores the database to the status when a specified log was generated.	· Use Differential: Turn on this switch if you want to use differential backup or incremental backup to restore the database. If you turn off this switch, HBR uses log backup to restore the database. · Use Log Area: specifies whether to initialize a log area. If you turn on this switch, you initialize the log area and cannot use log entries in this log area. Set this parameter as required. You can turn on this switch when the log area is unavailable, or you want to restore the database to a different system. · Validate Differential and Log: If you turn on this switch, HBR checks the availability of the required differential backup and log backup when the restoration job starts. If the differential backup or the log backup is unavailable, HBR stops the restoration job until the backup data is available. · Log Position: Specify the log generated in the status that you want to restore the database to. · Volume ID: Specify the ID of the volume to be restored.

8. Click Next.
9. Specify a backup as the reference. Then, click Create.

Related operations

In the HBR console, you can view the status of restoration jobs and cancel ongoing restoration jobs. The procedure is as follows:

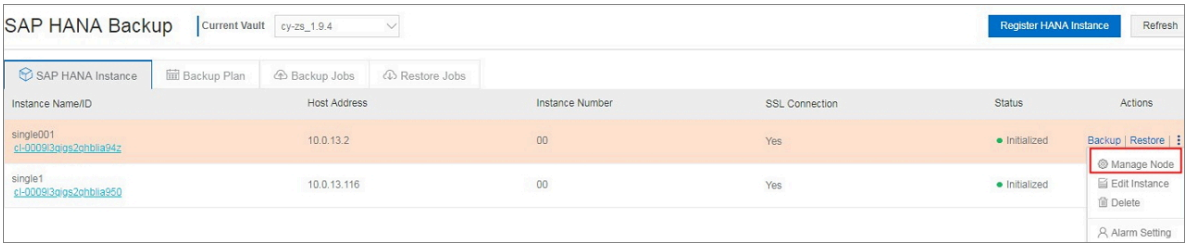
1. Log on to the HBR console.
2. In the left-side navigation pane, choose ECS Backup > SAP HANA Backup.
3. Click the Restore Jobs tab.
4. View the restoration job status on the Restore Jobs tab.
5. To cancel an ongoing restoration job, click Cancel in the right-side Actions column for the job.

2.5 Set a log backup policy

Hybrid Backup Recovery (HBR) supports log backup. This feature allows you to restore a database to the status at a specified time point.

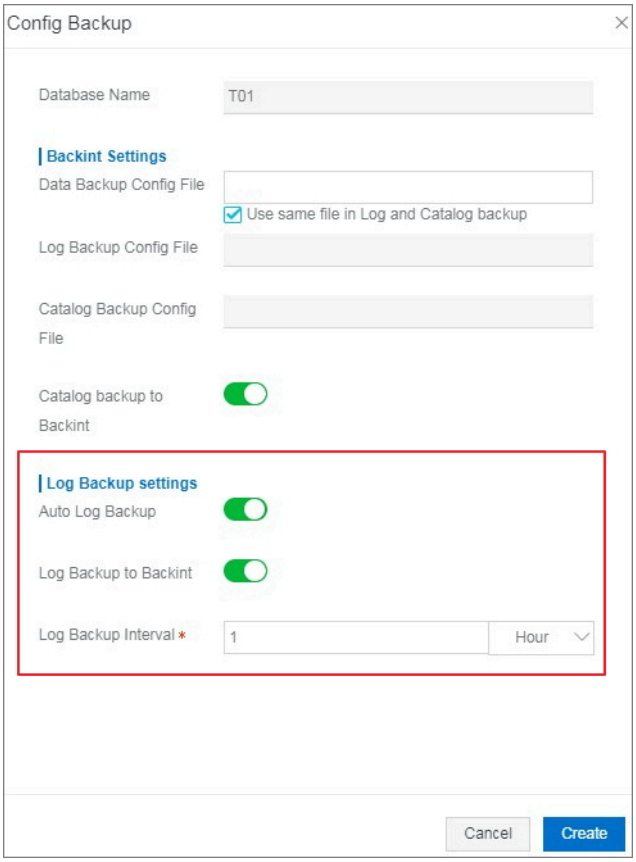
Procedure

1. Ensure that the SAP HANA instance is registered. On the SAP HANA Backup page, click the SAP HANA Instance tab.
2. In the `Actions` column, choose More > Manage Node for the target SAP HANA instance.



3. Click the Database tab to view the status of all databases on the SAP HANA instance.
4. In the right-side Actions column, choose More > Config Backup for the target database.

5. In the Config Backup dialog box, set the parameters as instructed in the following table.



Parameter	Description
`Auto Log Backup`	Specify whether to regularly back up logs.
`Log Backup to Backint`	Specify whether to use Backint to back up logs.
`Log Backup Interval`	Specify the interval for log backup. Minimum interval: 15 minutes.

6. Click Create.

2.6 Configure a backup profile

To perform a system copy, you need to create a backup profile and add its file path to the Hybrid Backup Recovery (HBR) backup configuration.

Note:

- We recommend that you use the created backup profile for both log backup and catalog backup.

- If an SAP HANA instance has multiple nodes, you must configure a backup profile for each node.
- After you create a backup profile, you need to configure the read and write permissions (permission 664) for the backup profile.

Create a backup profile

The procedure is as follows:

1. Create the */ usr / sap /< SID >/ SYS / global / hdb / opt / hdbconfig* directory.
2. Run the following command to create a backup profile in the specified directory:

```
vi  / usr / sap /< SID >/ SYS / global / hdb / opt / hdbconfig /
param
```

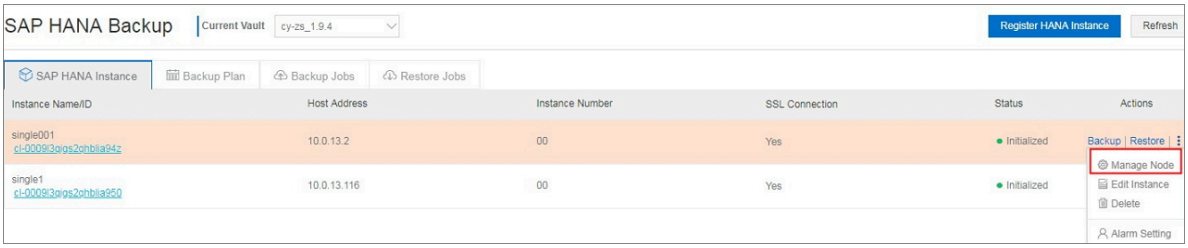
File parameters

Parameter	Description	Example
srcClusterId	The ID of the SAP HANA instance, which is generated by HBR when you register the SAP HANA instance.	i-bp14wddpc7 t2p7nrkk03
srcSID	The system ID of the source SAP HANA database.	T01

Add the file path of the backup profile

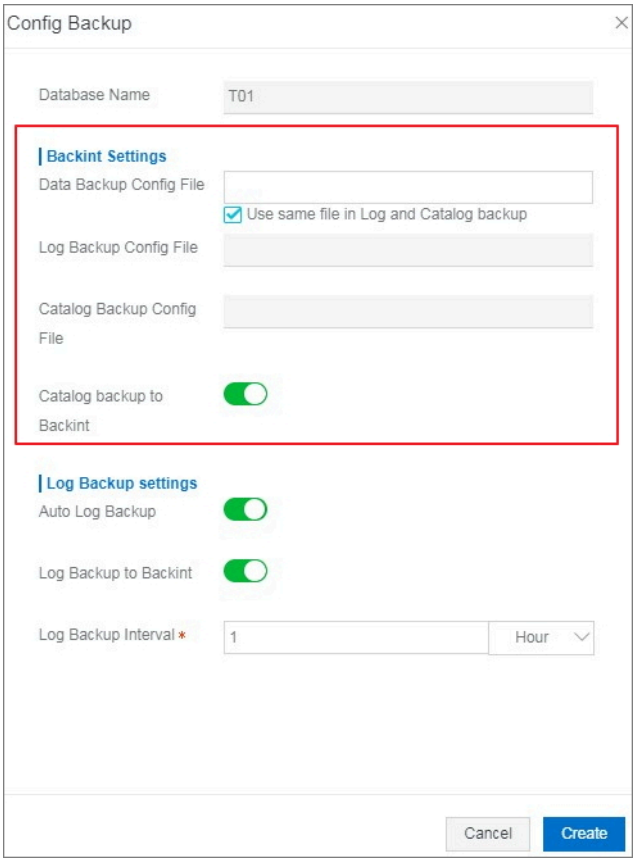
After creating a backup profile, you need to log on to the HBR console and add the file path to the HBR backup configuration. The procedure is as follows:

1. Ensure that the SAP HANA instance is registered. On the SAP HANA Backup page, click the SAP HANA Instance tab.
2. In the right-side `Actions` column, choose More > Manage Node for the target SAP HANA instance.



3. Click the Database tab to view the status of all databases on the SAP HANA instance.

4. In the right-side Actions column, choose More > Config Backup for the target database.
5. In the Config Backup dialog box, set the parameters as instructed in the following table.



Parameter	Description
Data Backup Config File	Specify the Backint parameter file for data backup.
Use same file in Log and Catalog backup	Select this check box to use the backup profile for both log backup and catalog backup. We recommend that you select this check box.
Log Backup Config File	Specify the Backint parameter file for log backup.
Catalog Backup Config File	Specify the Backint parameter file for catalog backup.
Catalog backup to Backint	Turn on this switch to use Backint to back up catalogs. We recommend that you enable this feature to improve the backup performance.

6. Click Create.

2.7 Backup alerts

Backup alerts provide you with alerts, such as when a backup fails or a client is disconnected from a server. By default, alerts are sent to an Alibaba Cloud account. You can also configure contacts, contact groups, and contact methods.

> Note:
> One hour after a backup fails or a client is disconnected from a server, the specified contact will receive an alert.

Configure alert contacts

An alert contact is a person who is assigned to receive backup alerts. You can add an alert contact in the HBR console. The procedure is as follows:

1. Log on to the HBR console.
2. In the left-side navigation pane, click Alarm Contact.
3. On the Alarm Contact Management page, click the `Alarm Contact` tab.
4. Click New Contact in the upper-right corner.
5. In the New Contact dialog box, set `Contact Name` .
6. Set `Contact Method` as required, and then perform the following operations:
   - Email

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

     If you select Mobile as a contact method, enter a mobile number in the Mobile field, and click Send Verification. An SMS message that contains a verification code is sent to your mobile phone. Enter the verification code in the `Mobile Verificati on Code` field.
7. Click OK.

> Note:
> - On the Alarm Contact tab, you can view a list of all alert contacts and their contact information.

- You can click Edit to modify the email address and mobile number of an alert contact.
- You cannot delete an alert contact who is specified to receive alert notifications or added to an alert contact group.

Configure alert contact groups

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, click Alarm Contact.
3. On the Alarm Contact Management page, click the `Alarm Contact Group` tab.
4. Click New Contact Group in the upper-right corner.
5. In the New Contact Group dialog box, set `Group Name` .
6. Select one or more alert contacts, and click  . These alert contacts are displayed in the `Selected Contact` section.
7. Click OK.

Note:

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

Customize alert policies

You can customize the following types of alert policies:

Note:

By default, HBR sends alert notifications by SMS or email to the alert contact specified in your Alibaba Cloud account. If you customize alert policies, the instance-level alert policy takes precedence over the vault-level alert policy.

- Vault-level alert policy

  A vault-level alert policy applies to all the backup clients of a vault. The backup clients include those installed on Alibaba Cloud Elastic Compute Service (ECS) instances, local hosts, and local virtual machines.

  Set a vault-level alert policy as follows:

  1. Log on to the HBR console.
  2. On the Overview page, find the vault for which you need to set an alert policy.
  3. In the upper-right corner of a vault card, click the Settings icon.
  4. In the Vault Setting dialog box, set `Alarm Policy` as required.
     - Disabled

       If you select this option, HBR does not send an alert notification when an alert is generated for a backup client or an instance that is related to the vault.
     - Default Notification

       If you select this option, HBR sends alert notifications by SMS or email to the alert contact specified in your Alibaba Cloud account when backup alerts are generated for the vault.
     - Customized Notification

       If you select this option, you can specify one or more alert contacts or alert contact groups. Then, HBR sends alert notifications to the specified alert contacts or alert contact groups when backup alerts are generated for the vault.
  5. Click OK.

- Instance-level alert policy

  An instance-level alert policy applies to all ECS backup clients of an SAP HANA instance.

  Set an instance-level alert policy as follows:

  1. Log on to the HBR console.
  2. Find the SAP HANA instance for which you need to set an alert policy. In the right-side Actions column, click Alarm Setting for the instance.
  3. In the Alarm Policy dialog box, set `Alarm Policy` as required.

Alarm policy	Description
`Disabled`	If you select this option, HBR does not send an alert notification when an alert is generated for the SAP HANA instance.
`Same as Vault`	If you select this option, the alert policy of the vault where the SAP HANA instance is located applies to the instance.
`Default Notification`	If you select this option, HBR sends alert notifications by SMS or email to the alert contact specified in your Alibaba Cloud account when backup alerts are generated for the SAP HANA instance.
`Customized Notification`	If you select this option, you can specify one or more alert contacts or alert contact groups. Then, HBR sends alert notifications to the specified alert contacts or alert contact groups when backup alerts are generated for the SAP HANA instance.

  4. Click OK.

3 Back up SQL Server databases in ECS

3.1 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 an Alibaba Cloud Elastic Compute Service (ECS) backup client for HBR to back up SQL Server databases deployed on ECS instances and restore these databases as required.

For more information about how to back up SQL Server databases, see the following topics:

- Preparations
- Back up a SQL Server database
- Restore a SQL Server database

For more information about other features of SQL Server database backup, see the following topic:

Configure the backup alerting feature

Note:

For more information about how to back up SQL Server databases deployed in a local IDC, see Workflow-based backup.

3.2 Preparations

You can use Hybrid Backup Recovery (HBR) to back up SQL Server databases deployed on Alibaba Cloud Elastic Compute Service (ECS) instances and restore these databases as required. This topic describes the preparations that you need to make before backing up data.

Note:

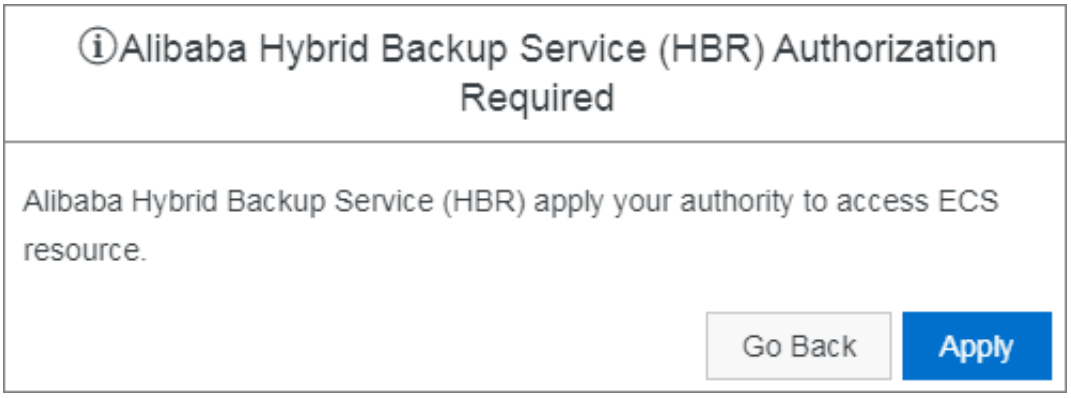
HBR supports the following SQL Server versions: SQL Server 2008 R2, SQL Server 2012, SQL Server 2014, SQL Server 2016, and SQL Server 2017. For more information, see Limits.

SQL Server databases cannot be installed in a file system where compression is enabled. For more information about SQL Server installation limits, see File Locations for Default and Named Instances of SQL Server.

Authorize roles

Before using HBR to back up files from ECS instances, you must authorize two roles AliyunHBRDefaultRole and AliyunECSAccessingHBRRole to access your cloud resources. The procedure is as follows:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose ECS Backup > ECS File Backup. Authorization dialog boxes appear one by one. Follow instructions to authorize the two roles to access your cloud resources.



Install Cloud Assistant

- An ECS backup client must work with Cloud Assistant. By default, a Cloud Assistant client is installed on ECS instances that are created after December 1, 2017. To back up files from ECS instances that you bought before December 1, 2017, you must install a Cloud Assistant client.
- When a Cloud Assistant client is installed on an ECS instance that is located on a classic network, you need to perform the following operations to configure the Cloud Assistant client based on the operating system of the ECS instance.
  - Windows:
    1. Connect to the ECS instance. In the `C:\ProgramData\aliyun\assist\` directory, create a file named `region-id` and enter the `region ID` in the file based on the region where the ECS instance is

located. For example, for an ECS instance that is located in China (Hangzhou), you need to enter `cn - hangzhou`.

```
C:\Users\Administrator>echo cn-hangzhou >C:\ProgramData\aliyun\assist\region-id
```

The following table lists regions and their region IDs.

Region	Region ID
China (Hangzhou)	cn-hangzhou
China (Shanghai)	cn-shanghai
China (Beijing)	cn-beijing
China (Shenzhen)	cn-shenzhen

2. Restart AliyunService in Task Manager.

- Linux:

1. Connect to the ECS instance. In the */ usr / local / share / aliyun - assist /* directory, create a file named `region - id` and enter the `region ID` in the file based on the region where the ECS instance is located. For example, for an ECS instance that is located in China (Hangzhou), you need to enter `cn - hangzhou`.

```
iZbp13t3ieoekp8ysnexhcZ:/ #
iZbp13t3ieoekp8ysnexhcZ:/ # echo cn-hangzhou >/usr/local/s
iZbp13t3ieoekp8ysnexhcZ:/ #
```

The following table lists regions and their region IDs.

Region	Region ID
China (Hangzhou)	cn-hangzhou
China (Shanghai)	cn-shanghai
China (Beijing)	cn-beijing
China (Shenzhen)	cn-shenzhen

2. To restart the Cloud Assistant client, run the `chkconfig agentwatch off` command and then the `chkconfig agentwatch on` command.

Alternatively, you can run the `systemctl restart agentwatch` command.

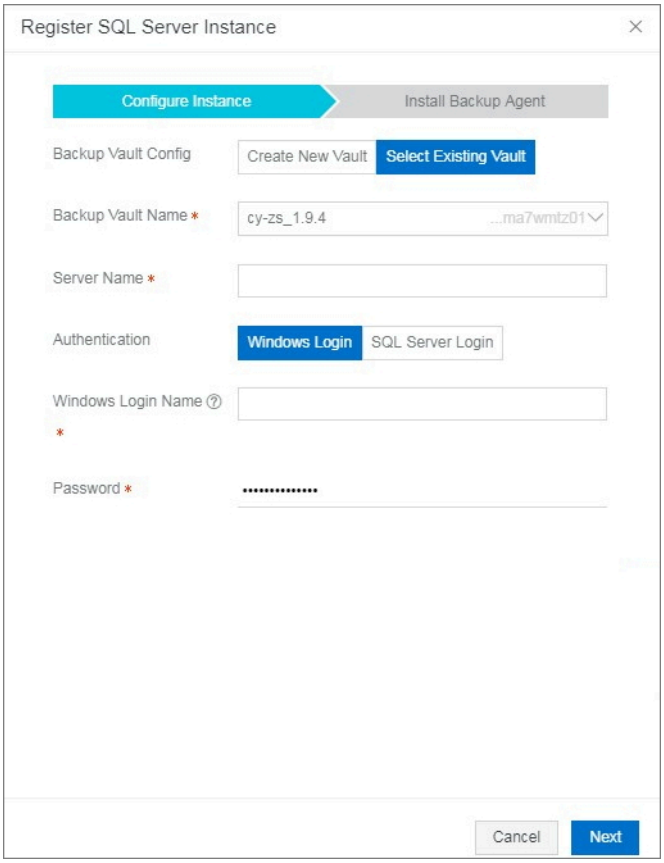
> Note:
> If the Cloud Assistant client still does not work after the restart, you need to run the preceding commands to restart it again.

Register a SQL Server instance

When you register a SQL Server instance, you need to configure the connection information about the SQL Server instance. After the SQL Server instance is registered, an ECS backup client is installed on each node of the SQL Server instance. The procedure is as follows:

1. Log on to the HBR console.
2. In the upper-left corner of the page, select a region where ECS instances that you need to back up are located.
3. In the left-side navigation pane, choose ECS Backup > SQL Server Backup.
4. In the upper-right corner, click Register SQL Server Instance.

5. In the Register SQL Server Instance dialog box, set the parameters as instructed in the following table.



Parameter	Description
Backup Vault Name	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. · If you have created backup vaults: Click Select Existing Vault and select a vault from the drop-down list. · If you have not created any backup vaults: Click Create New Vault, and then set Backup Vault Name and Vault Description to create a vault. The vault name cannot exceed 64 bytes in length.
Server Name	Specify the name of the server where the SQL Server instance is located.
Authentication	Select an authentication method for connecting to the SQL Server instance.

Parameter	Description
Windows Login Name	If you select Windows Login , enter the username used to log on to the SQL Server instance in Windows in the Windows Login Name field.
SQL Server User	If you select SQL Server Login , enter the username used to log on to the SQL Server instance in the SQL Server User field.
Password	Enter the password used to log on to the SQL Server instance based on the selected authentication method.

6. Click Next.
7. Select all ECS instances where the SQL Server instance is deployed so that HBR can install an ECS backup client on these ECS instances. In the drop-down list on the left of the search box, select Instance ID or Instance Name as the keyword. Enter a complete or partial ID or name in the search box to search for ECS instances.

   Note:
   If you select an ECS instance that is located on a classic network , you must enter the AccessKey ID and AccessKey secret.
8. Click Create. HBR automatically installs an ECS backup client on the selected ECS instances.

   Note:
   After the SQL Server instance is registered, you can click the SQL Server Instance tab on the SQL Server Backup page. On this tab, you can view the registration information and status of the registered SQL Server instance. In the right-side Actions column, you can choose More > Edit Instance to modify the SQL Server instance.

View and manage clients

After the SQL Server instance is registered, you can view the installation status of the ECS backup client on each node of the SQL Server instance. You can also install an ECS backup client on newly added nodes.

Install a client on a new node

If an ECS instance is added to the SQL Server cluster, you can install an ECS backup client on this ECS instance. The procedure is as follows:

1. Find the target SQL Server instance. Click the instance name or ID, or click View Detail for the instance in the right-side Actions column. The SQL Server Instance page appears.
2. Click the Client tab. In the upper-right corner of the Client tab, click Create Client.
3. Select the new ECS instance so that HBR can install an ECS backup client on this ECS instance. In the drop-down list on the left of the search box, select Instance ID or Instance Name as the keyword. Enter a complete or partial ID or name in the search box to search for this ECS instance.

    Note:
   If you select an ECS instance that is located on a `classic network`, you must enter the AccessKey ID and AccessKey secret.
4. Click OK.

Check the client installation status

To check the installation status of the ECS backup client on a node, perform the following operations:

1. Ensure that the SQL Server instance is registered. On the SQL Server Backup page, click the SQL Server Instance tab.
2. Find the target SQL Server instance. Click the instance name or ID, or click View Detail for the instance in the right-side Actions column. The SQL Server Instance page appears.
3. Click the Client tab to view the installation status of the ECS backup client on nodes. If the ECS backup client is installed, the node status is Activated. The following table describes the operations that you can perform in this case.

Operation	Procedure
Reinstall a backup client	If the backup client fails to be installed on a node, choose More > Re-install in the right-side Actions column for the node.
Uninstall a backup client	To uninstall the backup client from a node, choose More > Uninstall Client in the right-side Actions column for the node.

Operation	Procedure
Delete a backup client	To uninstall the backup client from a node and delete the node, click Delete in the right-side Actions column for the node. Note: Before deleting a backup client, you need to ensure that the backup client has no backup job in the Running or Completed state.

View databases

You can view the databases of a SQL Server instance. The procedure is as follows:

1. Find the target SQL Server instance. Click the instance name or ID, or click View Detail for the instance in the right-side Actions column. The SQL Server Instance page appears.
2. Click the Database tab. On this tab, you can view the database information of the target SQL Server instance.

Create a backup database group

Before starting backup, you need to group databases by backup plan. The procedure is as follows:

Note:
If you want to back up a database separately, create a group exclusively for this database.

1. Log on to the HBR console.
2. In the left-side navigation pane, choose ECS Backup > SQL Server Backup.
3. Click the Database Group tab. In the upper-right corner of the tab, click Edit Database Group.
4. In the Edit Database Group dialog box, set `Group Name` and `Descriptio n`. Then, select one or more databases, and add them to the group.
5. Click OK.

3.3 Back up a SQL Server database

You can use Hybrid Backup Recovery (HBR) to back up SQL Server databases deployed on Alibaba Cloud Elastic Compute Service (ECS) instances and restore these databases as required. This topic describes how to back up a SQL Server database.

Prerequisites

Preparations are completed.

Procedure

1. Log on to the HBR console.
2. In the left-side navigation pane, choose ECS Backup > SQL Server Backup.
3. In the right-side Actions column, click Backup for the SQL Server instance to be backed up.
4. In the Create Plan dialog box, select the database to be backed up.
   - If you want to back up an existing database group, click Database Group, and select a database group.
   - If you want to back up a new database group, you need to first create a backup database group. Click Select Database, select databases that you want to back up, and then set `Group Name` to create a backup database group.
   - If you want to back up all databases, click All Database.

5. Click Next. On the tab that appears, set the parameters as instructed in the following table.

Parameter	Description
Backup Type	· Complete: backs up full data in the database. · Differential: backs up data modified after the last full backup. Note: - Before you start the first differential backup for a database, you need to perform a full backup. - After you restore a database, to perform a differential backup for the database, you need to perform a full backup first. · Log: backs up logs for the database. - Before you back up logs for a database for the first time , you need to perform a full backup. - After you restore a database, to back up logs for the database, you need to perform a full backup first.
Plan Name	Specify the name of the backup plan.
Start Time	Select the time to start backup. The time is accurate to seconds.
Plan Interval	Select the frequency of backups. The time is accurate to the hour. Note: The retention period for differential backup is the same as that for full back, and cannot be modified.
Retention	Select the retention period for backup. Minimum retention period: one day. Maximum retention period: five years.

6. After the configuration is completed, click OK.

Related operations

View and edit a backup plan

In the HBR console, you can view the information and status of created backup plans, and manage these backup plans. The procedure is as follows:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose ECS Backup > SQL Server Backup.

3. Click the Backup Plan tab.
4. Check the backup plan information and status on the Backup Plan tab.
5. Click an operation in the Actions column to manage a backup plan. Operations in the Actions column are Edit, Excute Now, Disable Plan, Enable Plan, and Delete Plan. After you delete a backup plan, HBR does not run the plan any more but reserves backup data.

View and cancel a backup job

You can view the status of backup jobs. You can also cancel an ongoing backup job. The procedure is as follows:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose ECS Backup > SQL Server Backup.
3. Click the Backup Jobs tab.
4. Check the backup job information and status on the Backup Jobs tab.
5. To cancel an ongoing backup job, click Cancel in the right-side Actions column for the job.

View the history of database backup and log backup

You can view the history of database backup and log backup. The procedure is as follows:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose ECS Backup > SQL Server Backup.
3. Click the SQL Server Instance tab.
4. Find the target SQL Server instance. Click the instance name or ID, or click View Detail for the instance in the right-side Actions column. The SQL Server Instance page appears.
5. On the SQL Server Instance page, click the Data Backups tab to view database backup records, or the Log Backups tab to view log backup records.

3.4 Restore a SQL Server database

After using Hybrid Backup Recovery (HBR) to back up SQL Server databases to a backup vault, you can restore the SQL Server databases to the original SQL Server instance or another SQL Server instance that uses the same backup vault.

Note:

- When you choose to restore a SQL Server database from incremental backup, HBR automatically uses full backup to restore the database before using incremental backup.
- To restore the primary database of a SQL Server instance, you need to start the SQL Server instance in single-user mode.
- To restore the databases of a SQL Server instance to another SQL Server instance, ensure that the source SQL Server instance version is not later than the destination SQL Server instance version.

Procedure

1. Log on to the HBR console.
2. In the left-side navigation pane, choose ECS Backup > SQL Server Backup.
3. Click the SQL Server Instance tab.
4. Find the SQL Server instance to be restored, and click Restore in the right-side `Actions` column.
5. In the New Restore Task dialog box, select the source SQL Server instance and click Next.

6. Select a database to be restored, and click Next. Then, set restoration rules as instructed in the following table.

Parameter	Description
Destination Database	Specify the name of the database restored on the destination SQL Server instance.  Note: · If you want to use the restored database to overwrite an existing database, enter the name of the existing database in this field, and then select Override existing database. · Otherwise, do not enter a name that is the same as that of any existing databases.
Restore Policy	· Most Recent Restores the database to the latest available status. · Time Point Restores the database to the status closest to a specified time point. After selecting this option, you need to specify a time point. · From Snapshot Restores the database to a specified backup. After selecting this option, you need to specify a backup.

7. Click Next, confirm the configuration, and then click Create.

View and cancel restoration jobs

In the HBR console, you can view the status of restoration jobs and cancel ongoing restoration jobs. The procedure is as follows:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose ECS Backup > SQL Server Backup.
3. Click the Restore Jobs tab.
4. View the restoration job status on the Restore Jobs tab.
5. To cancel an ongoing restoration job, click Cancel in the right-side Actions column for the job.

3.5 Backup alerts

Backup alerts provide you with alerts, such as when a backup fails or a client is disconnected from a server. By default, alerts are sent to an Alibaba Cloud account. You can also configure contacts, contact groups, and contact methods.

> Note:
> One hour after a backup fails or a client is disconnected from a server, the specified contact will receive an alert.

Configure alert contacts

An alert contact is a person who is assigned to receive backup alerts. You can add an alert contact in the HBR console. The procedure is as follows:

1. Log on to the HBR console.
2. In the left-side navigation pane, click Alarm Contact.
3. On the Alarm Contact Management page, click the `Alarm Contact` tab.
4. Click New Contact in the upper-right corner.
5. In the New Contact dialog box, set `Contact Name` .
6. Set `Contact Method` as required, and then perform the following operations:
   - Email

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

     If you select Mobile as a contact method, enter a mobile number in the Mobile field, and click Send Verification. An SMS message that contains a verification code is sent to your mobile phone. Enter the verification code in the `Mobile Verificati on Code` field.
7. Click OK.

> Note:
> - On the Alarm Contact tab, you can view a list of all alert contacts and their contact information.

- You can click Edit to modify the email address and mobile number of an alert contact.
- You cannot delete an alert contact who is specified to receive alert notifications or added to an alert contact group.

Configure alert contact groups

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, click Alarm Contact.
3. On the Alarm Contact Management page, click the `Alarm Contact Group` tab.
4. Click New Contact Group in the upper-right corner.
5. In the New Contact Group dialog box, set `Group Name` .
6. Select one or more alert contacts, and click  . These alert contacts are displayed in the `Selected Contacts` section.
7. Click OK.

Note:

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

Customize alert policies

You can customize the following types of alert policies:

Note:

By default, HBR sends alert notifications by SMS or email to the alert contact specified in your Alibaba Cloud account. If you customize alert policies, the instance-level alert policy takes precedence over the vault-level alert policy.

- Vault-level alert policy

  A vault-level alert policy applies to all the backup clients of a vault. The backup clients include those installed on Alibaba Cloud Elastic Compute Service (ECS) instances, local hosts, and local virtual machines.

  Set a vault-level alert policy as follows:

  1. Log on to the HBR console.
  2. On the Overview page, find the vault for which you need to set an alert policy.
  3. In the upper-right corner of a vault card, click the Settings icon.
  4. In the Vault Setting dialog box, set `Alarm Policy` as required.
     - Disabled

       If you select this option, HBR does not send an alert notification when an alert is generated for a backup client or an instance that is related to the vault.
     - Default Notification

       If you select this option, HBR sends alert notifications by SMS or email to the alert contact specified in your Alibaba Cloud account when backup alerts are generated for the vault.
     - Customized Notification

       If you select this option, you can specify one or more alert contacts or alert contact groups. Then, HBR sends alert notifications to the specified alert contacts or alert contact groups when backup alerts are generated for the vault.
  5. Click OK.

- Instance-level alert policy

  An instance-level alert policy applies to all ECS backup clients of an SAP HANA instance.

  Set an instance-level alert policy as follows:

  1. Log on to the HBR console.
  2. Find the SAP HANA instance for which you need to set an alert policy. In the right-side Actions column, click Alarm Setting for the instance.
  3. In the Alarm Policy dialog box, set `Alarm Policy` as required.

Alarm policy	Description
`Disabled`	If you select this option, HBR does not send an alert notification when an alert is generated for the SAP HANA instance.
`Same as Vault`	If you select this option, the alert policy of the vault where the SAP HANA instance is located applies to the instance.
`Default Notification`	If you select this option, HBR sends alert notifications by SMS or email to the alert contact specified in your Alibaba Cloud account when backup alerts are generated for the SAP HANA instance.
`Customized Notification`	If you select this option, you can specify one or more alert contacts or alert contact groups. Then, HBR sends alert notifications to the specified alert contacts or alert contact groups when backup alerts are generated for the SAP HANA instance.

  4. Click OK.