Alibaba Cloud Hybrid Backup

Back up on-premises severs

Issue: 20190814

MORE THAN JUST CLOUD | 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 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 for on-premises severs

1.1 Overview

Hybrid Backup Recovery (HBR) is an efficient, secure, cost-effective, and fully managed storage and backup service. You can use a file client to back up files from servers or virtual machines that are located in local data centers. You can quickly restore files when one or more files are missing or damaged.

This topic includes the following sections:

- Prerequisites
- Start a backup job
- Restore files

The following functions are related to this topic:

- Search backups
- Backup alerts
- Mirror vaults

Note:
For more information, see Back up files from ECS instances.

1.2 Prerequisites

You can use Hybrid Backup Recovery (HBR) to back up files and folders from servers or virtual machines in local data centers and restore these files as required. The following prerequisites are required before you back up data.

Note:

- For more information, see Back up files from an ECS instance.
- 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 of 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.

RAM users and AccessKeys

Resource Access Management (RAM) enables you to manage user access to Alibaba Cloud resources. You can create and manage multiple RAM users with a single Alibaba Cloud account. You can grant different permissions for each RAM user. This allows each RAM user to have different access permissions on Alibaba Cloud resources.

An AccessKey is required when you activate a backup client. As any leak of an Alibaba Cloud account's AccessKey will expose cloud resources to security risks, we recommend that you use the AccessKey of a RAM user to perform the activation. Before performing a backup job, ensure that you have Created a RAM user and Created an access key for a RAM user.

Create a client

You can use a file client to perform a backup or restore job. However, you must download a file client to a host that is located in a local data center. You can download a file client in the HBR console. Proceed as follows:

1. Log on to the HBR console.

   Note:
   You must log on to the HBR console on an intermediate host with a desktop environment to download a file client. You need to perform this operation if a server or virtual machine where a Linux system is running but without a desktop environment.

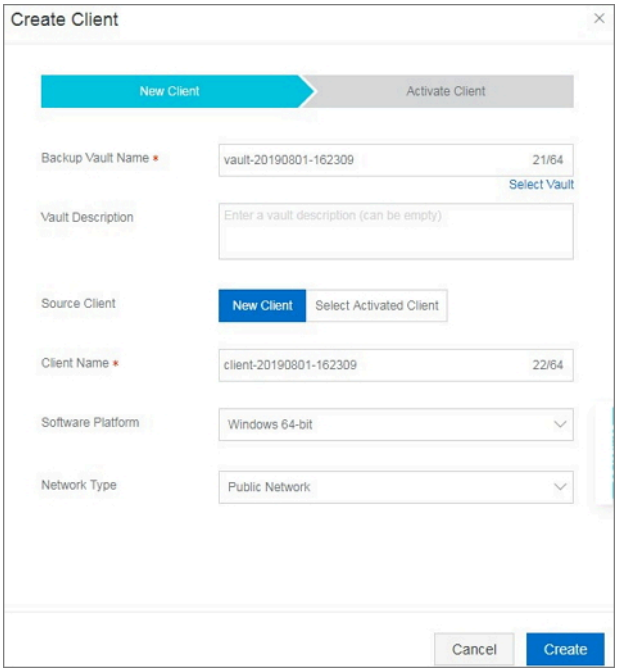
2. At the top of the HBR console, select a region where you need to store backups.

   Note:

   - If a VPC is used, the region you select must be the same as the region of the VPC where data to be backed up is located.
   - For optimal backup performance, you must select a region that is in close proximity to the location where data to be backed up is located.

- For disaster recovery, you must select a different region for the location where data to be backed up is located. We recommend that you select a distant region to reduce the risk of data loss during a disaster.

3. In the left-side navigation pane, choose On-Premises Backup > File Client.
4. In the upper-right corner of the page, click Create Client.
5. In the Create Client dialog box, configure the required settings and click Create. Settings are described in the following table.



Name	Description
Backup Vault Name	A backup vault is an HBR cloud backup warehouse used to store backup data on the cloud. Backup data from multiple clients can be stored in the same vault. · One or more backup vaults available You can select a backup vault on the drop-down list. · No backup vault available Click Create Vault. Enter the Backup Vault Name and Vault Description to create a new backup vault. The vault name must be a maximum of 64 characters in length.
Client Name	The name of the backup client. The client name must be a maximum of 64 characters in length.

Name	Description
Software Platform	The operating system that is running on the host from which you need to back up data. Valid values: · Windows 32-bit · Windows 64-bit · Linux 32-bit · Linux 64-bit
Network Type	· `Virtual Private Cloud (VPC)`: Select this option when the host to be backed up is located in a VPC and in the same region where the backup vault is located. · `Public Network`: Select this option when VPCs are not applicable.

6. Click Create and then click Download Client.

 Note:
You can install a client to connect a host to HBR. You can also go to the File Client page and download a client at any time.

Install and activate a client

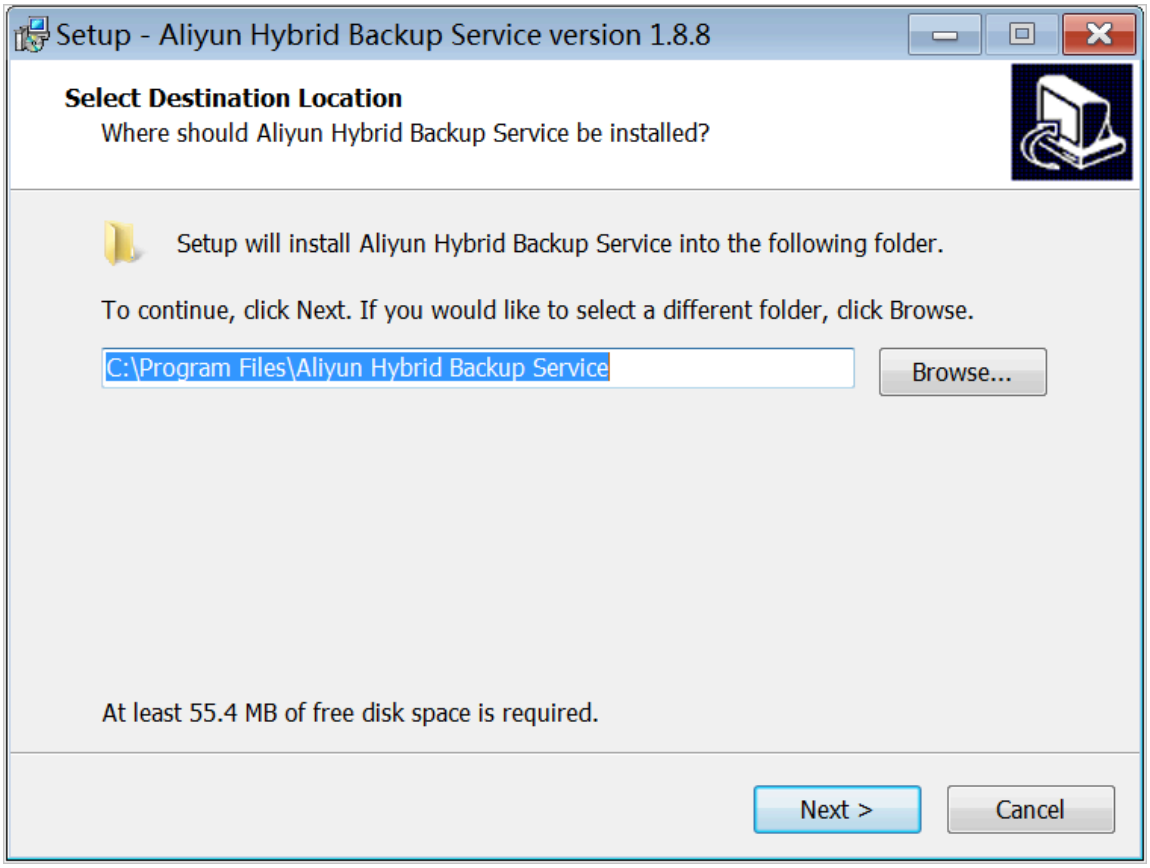
After you download a file client, you need to install and activate the client. Proceed as follows:

1. Install a client from an installation package and select an installation folder.

 Note:

As operation logs and executable files are all stored in the installation folder, you must ensure that the installation folder contains sufficient available space.

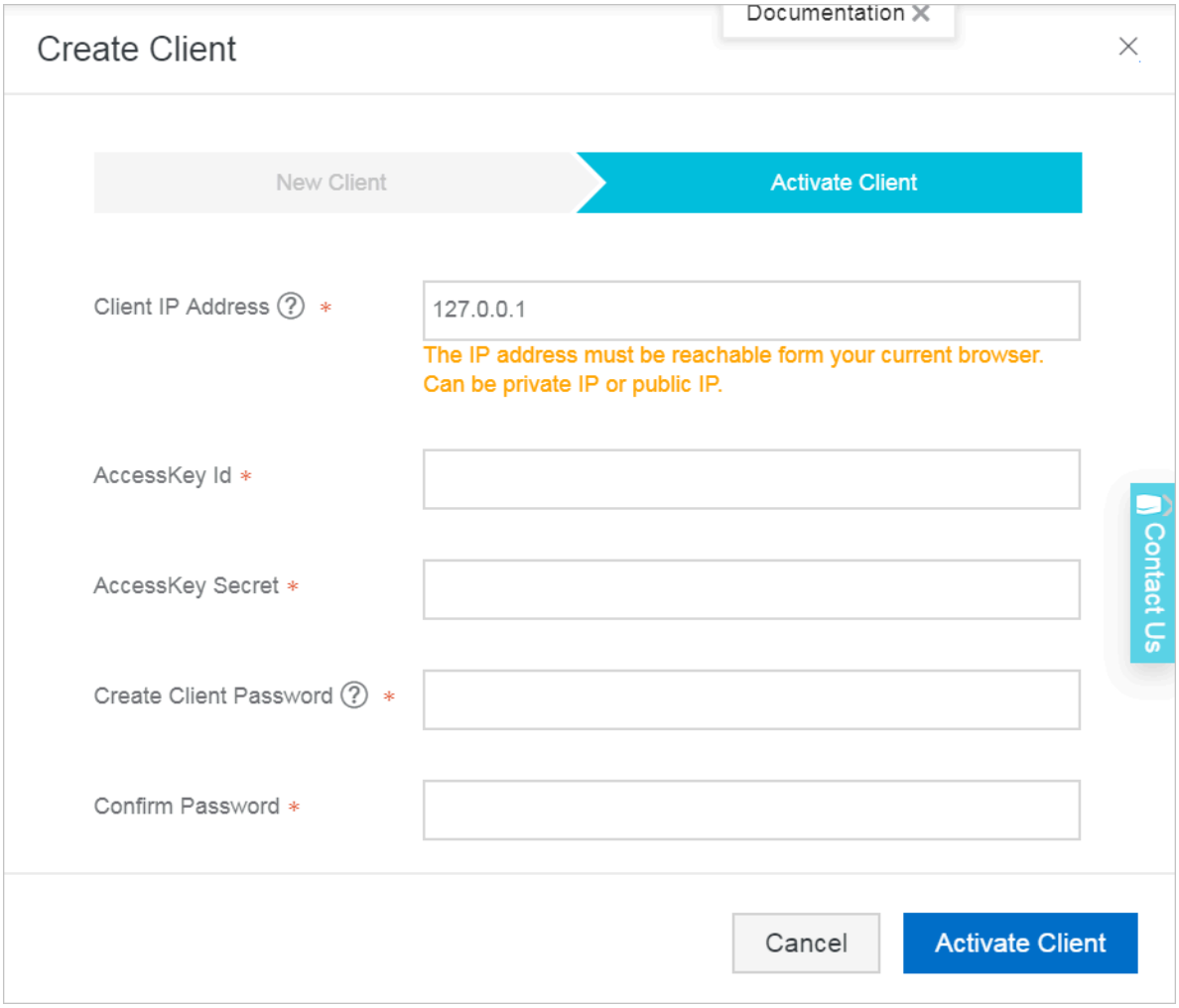
- If you install a client on Windows, run an installation package, select an installation folder, and follow the instructions to complete the installation.



- If you install a client on Linux, extract an installation package to a folder and run the `./ setup` command to install the client.

```
[root@47 software]# tar -zxvf hbr-install-1.3.4-linux-amd64.tar.gz
hbr-install-1.3.4-linux-amd64/
hbr-install-1.3.4-linux-amd64/client/
hbr-install-1.3.4-linux-amd64/download/
hbr-install-1.3.4-linux-amd64/logs/
hbr-install-1.3.4-linux-amd64/setup
hbr-install-1.3.4-linux-amd64/uninstall
hbr-install-1.3.4-linux-amd64/update/
hbr-install-1.3.4-linux-amd64/versions/
hbr-install-1.3.4-linux-amd64/update/updater
hbr-install-1.3.4-linux-amd64/client/hybridbackup
hbr-install-1.3.4-linux-amd64/client/ids
hbr-install-1.3.4-linux-amd64/client/resource/
hbr-install-1.3.4-linux-amd64/client/www/
hbr-install-1.3.4-linux-amd64/client/www/dist/
hbr-install-1.3.4-linux-amd64/client/www/dist/index.html
hbr-install-1.3.4-linux-amd64/client/www/dist/static/
hbr-install-1.3.4-linux-amd64/client/www/dist/static/css/
hbr-install-1.3.4-linux-amd64/client/www/dist/static/fonts/
hbr-install-1.3.4-linux-amd64/client/www/dist/static/img/
hbr-install-1.3.4-linux-amd64/client/www/dist/static/js/
hbr-install-1.3.4-linux-amd64/client/www/dist/static/js/app.7e558a4017f7c8ad58a4.js
hbr-install-1.3.4-linux-amd64/client/www/dist/static/js/manifest.afb9fdc23e85cda133f8.js
hbr-install-1.3.4-linux-amd64/client/www/dist/static/js/vendor.cbd4977a3094b35cf5a3.js
hbr-install-1.3.4-linux-amd64/client/www/dist/static/img/hbr_logo.b8bbcfb.png
hbr-install-1.3.4-linux-amd64/client/www/dist/static/img/logo.1922e1b.png
hbr-install-1.3.4-linux-amd64/client/www/dist/static/img/logotxt.827883a.png
hbr-install-1.3.4-linux-amd64/client/www/dist/static/img/logotxt_en.eefd9c8.png
hbr-install-1.3.4-linux-amd64/client/www/dist/static/fonts/element-icons.6f0a763.ttf
hbr-install-1.3.4-linux-amd64/client/www/dist/static/fonts/iconfont.012cf6a.woff
hbr-install-1.3.4-linux-amd64/client/www/dist/static/fonts/iconfont.a24068e.woff2
hbr-install-1.3.4-linux-amd64/client/www/dist/static/fonts/iconfont.a37b0c0.ttf
hbr-install-1.3.4-linux-amd64/client/www/dist/static/css/app.2af72af1fc9bac8fc91108877b2708bc.css
hbr-install-1.3.4-linux-amd64/client/resource/en-US.json
hbr-install-1.3.4-linux-amd64/client/resource/zh-CN.json
[root@47 software]# cd hbr-install-1.3.4-linux-amd64
[root@47 hbr-install-1.3.4-linux-amd64]# ll
total 28
drwxr-xr-x 4 501 games 4096 Sep 21 16:31 client
drwxr-xr-x 2 501 games 4096 Sep 12 10:36 download
drwxr-xr-x 2 501 games 4096 Sep 12 10:36 logs
-rwxr-xr-x 1 501 games  307 Sep 12 10:36 setup
-rwxr-xr-x 1 501 games  233 Sep 12 10:36 uninstall
drwxr-xr-x 2 501 games 4096 Sep 21 16:31 update
drwxr-xr-x 2 501 games 4096 Sep 12 10:36 versions
[root@47 hbr-install-1.3.4-linux-amd64]# ./setup
Setting up Hybrid backup client ...
Complete
[root@47 hbr-install-1.3.4-linux-amd64]#
```

2. After a client is installed, you need to activate the client. Go to the HBR console, in the Create Client dialog box, click Next and configure the required settings as described in the following table to activate the client.



Note:
We recommend that you download and install a client before activating the client.

Name	Description
Client IP Address	The IP address of the file client, which must be accessible by the host. The IP address is either an internal IP address or a public IP address. For example, 127.0.0.1 (default), 12.34.56.78:8011, and http://87.65.43.21:8443. **Note:** The IP address must be accessible by a browser.
AccessKey ID	Download the AccessKey ID and AccessKey Secret of the Alibaba Cloud account where the HBR service is activated.

Name	Description
AccessKey Secret	Download the AccessKey ID and AccessKey Secret of the Alibaba Cloud account where the HBR service is activated.
Create Client Password	Set the logon password of the client. The password must be a minimum of six characters in length.

3. Click Activate Client to open a web page. You can use this web page to manage the file client. You can use a file client to back up data.

> Note:
> If you fail to activate a client, you can reactivate the client.

(Optional) Create a backup plan and backup policy

Before you perform a backup job, we recommend that you schedule the backup time and interval of the backup job based on your business needs.

- If no regular backup plan exists, you can skip this step.
- If you have a regular backup plan, you can perform the following steps to create a backup policy and specify the first backup time and backup interval.

Procedure

1. Open a browser and enter `http :// localhost : 8011` in the address bar and enter the password to log on to an HBR file client.

> Note:
> - If you perform a backup operation on an intermediate host, you must change `localhost` to the IP address of the server or virtual machine from which you need to back up data.
> - Port 8011 is the default port that you can use to logon to a file client. If port 8011 on the server or virtual machine is occupied by another application, you can specify another port number for the file client.

2. In the left-side navigation pane, select Backup Policies.
3. On the Backup Polices page, click Create Policy.

4. In the Create Policydialog box, enter the `Name` , configure the required settings as described in the following table, and click Submit.

Name	Description
Name	The name of the policy.
Frequency	Unit: · Hour. Valid values: 1 to 23. · Day. Valid values: 1 to 6. · Week. Valid values: 1 to 4.
Backup Time	The first backup time. The first backup is a full backup.
Retention	· Unit: day, month, and year. · Maximum retention period: 3650 days (10 years).

Subsequent operations

Back up files from locate data centers

1.3 Backup files

You can use a Hybrid Backup Recovery (HBR) backup client to back up files and folders from a local server or virtual machine. HBR supports the following backup modes: instant backup and scheduled backup. You can select the required backup mode based on business needs.

Instant backup

If you have no regular backup plan and only need to perform a full backup, you can perform the following steps:

1. Log on to an HBR client.
2. On the Backup Jobs page, click Create Backup Job.

3. In the Create Backup Job dialog box, select the Basic Settings tab and configure the required settings as described in the following table.

Name	Description
Source	· The path of a backup source. You can enter a maximum of eight source paths, which means you can back up files from eight directories at a time. Separate source paths with carriage returns. · You can enter a Uniform Naming Convention (UNC) path as a source path.
Use VSS for backup (Windows only)	· If you need to ensure data consistenc y between a backup source and its backup when data changes occur in the backup source, you can select this option. · The feature is only available for hosts running Windows. · If you use Volume Shadow Copy (VSS), you cannot back up data from multiple directories at a time.
Running Plan	Select Instant.

4. (Optional) Select the Bandwidth Throttling tab. Specify the required Work Hours and click Add. Then, enter the maximum allowed bandwidth during the specified time range in the `Throttling` field.

Note:

- The unit of the throttling period is accurate to the hour. You can add multiple throttling periods based on actual needs.
- If you need to modify a throttling period, click Delete next to the throttling period and add a new throttling period.
- The maximum bandwidth must be more than or equal to 1 Mbit/s.

5. Click Submit to start the backup job.

Note:

After a backup job is started, you can perform the following actions on the Backup Jobs page:

- View the progress of the backup job.
- In the Actions column, cancel or retry the backup job.
- If a number of files failed to back up, locate the failed backup job on the `Backup Jobs` page. Click the Download icon next to the `number of failed files` to download the error report.

Scheduled backup

If you have a regular backup plan, you can create a scheduled backup based on a custom backup policy. Proceed as follows:

1. Log on to an HBR client.
2. In the left-side navigation pane, select Backup.
3. In the upper-right corner of the page, click Create Backup Job.
4. In the Create Backup Job dialog box, select the Basic Settings tab.
5. Enter the `Source` , select Scheduled, and select a `Backup Policy` .

Name	Description
Source	· 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. Separate source paths with carriage returns. · You can enter a Uniform Naming Convention (UNC) path as a source path.
Use VSS for backup (Windows only)	· If you need to ensure data consistenc y between a backup source and its backup when data changes occur in the backup source, you can select this option. · The feature is only available for hosts running Windows. · If you use Volume Shadow Copy (VSS), you cannot back up data from multiple directories at a time.

Name	Description
Running Plan	Select Scheduled.
Backup Policy	Select a backup policy from the drop-down list.

6. (Optional) Select the Bandwidth Throttling tab. Specify the required Working Hours and click Add. Then, enter the maximum allowed bandwidth during the specified time range in the `Throttling` field.

   Note:

   - The unit of the throttling period is accurate to the hour. You can add multiple throttling periods based on actual needs.
   - If you need to modify a throttling period, click Delete next to the throttling period and add a new throttling period.
   - The maximum bandwidth must be no less than 1 Mbit/s.

7. Click Submit.

Note:

After a backup job is started, you can perform the following actions on the Backup Jobs page:

- View the progress of the backup job
- In the Actions column, cancel or retry the backup job.
- In the Actions column, delete the backup job. After a backup job is deleted, the backup job is disabled and no backup policy applies to the backup job. However, backups that are created by the back job are retained and you can still restore data from these backups.
- If a number of files failed to back up, locate the failed backup job on the `Backup Jobs` page. Click the Download icon next to the `number of failed files` to download the error report.

1.4 Restore backups

You can restore backups to a server or virtual machine. This applies to backups that are created by using a client or another client in the same vault.

 Note:
When you restore a piece of data among a large number of backups, you can use theSearch backups function to locate the target piece of data in seconds.

Restore backups by using this client

Procedure

1. Log on to a Hybrid Backup Recovery (HBR) backup client.
2. In the left-side navigation pane, select Restore to open the Restore Backup / Backups page.
3. On the `Backups` tab, locate the target backup, and click Restore next to the backup.
4. In the Restore Backup dialog box, configure the required settings as described in the following table, select backups to be restored, and click Submit to restore these backups.

Name	Description
Target Folder	The target folder to which backups are restored.
File Options	· Include Files: Only selected files and folders are restored to the target folder. · Exclude Files: All files and folders are restored to the target folder except for the selected files and folders.

Restore from other clients

Procedure

1. Log on to an HBR client.
2. In the left-side navigation pane, select Restore to open the Restore Backup / Backups page.
3. In the upper-right corner of the page, click Restore From Other Client.

4. In the Restore Backup dialog box, select a client where files to be restored are located and click Next.
5. Select the version of a backup to be restored and click Next.
6. On the Restore File tab, configure the required settings as described in the following table, select files to be restored, and click Submit to restore a backup.

Name	Description
Target Folder	The target folder to which backups are restored.
File Options	· Include Files: Only selected files and folders are restored to the target folder. · Exclude Files: All files and folders are restored to the target folder except for the selected files and folders.

1.5 Search backups

When you restore a piece of data among a large number of backups, you can use the backup search function to locate the target piece of data in seconds.

Turn on the backup search function

1. Log on to the Hybrid Backup Recovery (HBR) console.
2. In the left-side navigation pane, select Overview.
3. On the Overview page, locate the required vault where you need to turn on the backup search function.
4. In the upper-right corner of the vault, click Settings.
5. In the Vault Setting dialog box, turn on `Backup Search`.

> Note:
> The backup search function is only available for vaults that are located in the China (Hangzhou) and China (Shanghai) regions.

Search backups

1. Log on to an HBR backup client.
2. In the left-side navigation pane, select Restore.
3. On the Restore Backup / Backups page, select the Search Backups tab.

4. Enter a keyword or relative path of a file that you need to restore and click Search.

   Note:

   - You can search for a file by using the full name of the file. You must enclose the full name with a pair of quotation marks (").
   - When searching for a file by a relative path, you must use forward slashes (/) as delimiters. For example, A/test.text.

5. You can also turn on Advanced Search in the upper-right corner of the page. Configure one or more of the following settings and click Search.

Name	Description
File Type	Select File or Folder as required.
Modify Time	The last modification time of a file. The time is accurate to the second. If you need to clear the specified time, click X next to the time.
File Size	You can specify a range of backup sizes. Valid values : KB, MB, and GB. The minimum size of a backup is 0 KB.
Backup Time	A time period in which the target backup is completed. You must specify the start time and the end time of the period. The time is accurate to the second. If you need to clear the specified time, click X next to the time.

   If you need to cancel the previous settings, click Reset.

6. Search results are displayed at the bottom of the Search Backups page, locate the backup you need to restore and click Restore next to the backup.
7. In the Restore Backup dialog box, enter the target folder to which you need to restore the file, and click Submit to restore the backup.

1.6 Backup alerts

Backup alerts provide you with alerts, such as when a backup fails or when a client is disconnected from a server. 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 selected to receive backup alerts. You can create an alarm contact as follows:

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` 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` as required, 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 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 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 contacts and the details of each contact.
- You can click Edit to modify the email and mobile number.
- You cannot delete a contact that is selected to receive alerts or added to a contact group.

Create an alarm contact group

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

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

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

Create custom alarm policies

You can create the following types of alarm policies:

- Vault-level alarm policies

  A vault-level alarm policy applies to all the backup clients of a vault. The backup clients include those installed on ECS instances, local hosts, and local virtual machines. If you create an alarm policy for the vault where a client is located, the alarm policy of the vault applies to the client by default.

- Client-level alarm policies

  A client-level alarm policy applies to the backup client installed on a specific host . After you create an alarm policy for a client, the client no longer uses the alarm policy of the vault or the default alarm policy.

 **Note:**
If you create no alarm policy for a vault or a client, alerts are sent to an Alibaba Cloud account by using emails.

Create a vault-level alarm policy

Proceed as follows:

1. Log on to the HBR console.
2. On the Overview page, locate the required vault to create an alarm policy.
3. In the upper-right corner of a vault, click Settings.
4. In the Vault Setting dialog box, select an `Alarm Policy` as required.
   - Disabled

     If you select this option, no alert is sent when an alarm occurs on a client or ECS instance that is located in the vault.
   - Default Notification

     If you select this option, alerts for the vault are sent to an Alibaba Cloud account by using emails.
   - Customized Notification

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

Create an alarm policy for a client

Proceed as follows:

1. Log on to the HBR console.
2. Locate a client to create an alarm policy, choose More > Alarm Setting next to the client.
3. In the Alarm Policy dialog box, select the required `Alarm Policy` .

Alarm Policy	Description
Disabled	If you select this option, no alert is sent when an alarm occurs on the client.

Alarm Policy	Description
Same as Vault	The alarm policy of the vault where the client is located applies to the client.
Default Notification	Alerts for the client are sent to an Alibaba Cloud account by using emails.
Customized Notification	You can select one or more contacts and contact groups. After you complete the configuration, alerts for the client are sent to the selected alarm contacts or alarm contact groups.

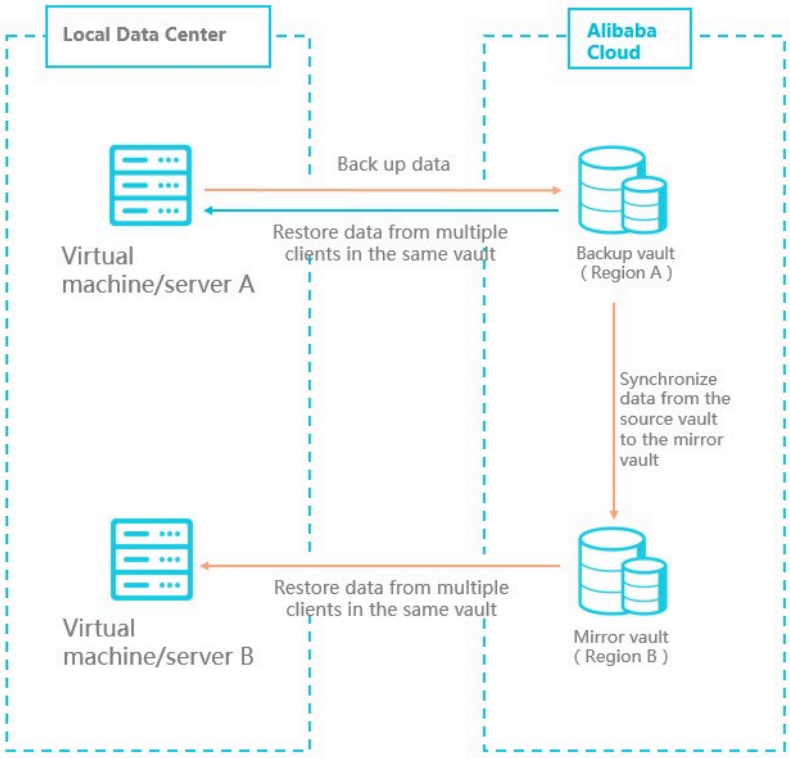
4. Click OK.

1.7 Mirror vaults

A backup vault is an HBR cloud backup warehouse used to store backup data on the cloud. You can create a remote mirror vault for a vault to meet disaster recovery requirements. You can also use a mirror vault for cross-region data restoration.

Note:

- After a mirror vault is created, backup jobs that are running in the source vault are synchronized to the mirror vault in real time. The historical backups of 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 from a mirror vault but cannot back up data to a mirror vault.
- You must delete a mirror vault before deleting the linked 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, click Overview.
3. Locate a vault for which you need 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, we recommend that you do not select the same region where the source vault is located.
5. Enter the `Vault Name`. The vault name must be a maximum of 32 characters in length.
6. Enter the `Vault Description` as required, and click Create.

Restore backups from mirror vaults

To restore data from a remote mirror vault, you need to download a backup client to the target server or virtual machine. You must specify the backup source as the mirror vault for the backup client. Proceed as follows:

1. On the server or virtual machine from which you need to restore data, download and install a backup client.

   
   Note:
   When you configure the backup client, you need to specify the `Backup Vault Name` as the name of the target mirror vault.

2. Log on to the backup client on the target server or virtual machine, and restore backups from another client.

   
   Note:
   You can also use the Search backups function to restore backups.

2 Back up virtual machine image

2.1 Overview

Hybrid Backup Recovery (HBR) is an efficient, secure, cost-effective, and fully managed backup and storage service. You can use HBR to back up the images of local virtual machines and restore these images as needed.

This topic includes the following sections:

- Prerequisites
- Back up data from a VMware virtual machine
- Restore data to a VMware virtual machine

The following sections are related to this topic:

Backup alerts

2.2 Prerequisites

Hybrid Backup Recovery (HBR) allows you to back up the images of local VMware vSphere virtual machines and restore these images as needed. The following prerequisites are required before you perform a backup job.

RAM users and AccessKeys

Resource Access Management (RAM) enables you to manage user access to Alibaba Cloud resources. You can create and manage multiple RAM users with a single Alibaba Cloud account. You can grant different permissions for each RAM user. This allows each RAM user to have different access permissions to Alibaba Cloud resources.

An AccessKey is required when you activate a backup client. As the leak of an Alibaba Cloud account's AccessKey exposes cloud resources to security risks, we recommend that you use the AccessKey of a RAM user to perform the activation. Before performing a backup job, ensure that you have Created a RAM user and Created an access key for a RAM user.

Create a client

You can use virtual machine clients to perform backup and restore jobs. You can perform the following steps to configure a backup client and download the backup client to a server where vSphere Client is installed:

1. On the server where vSphere Client is installed, log on to the HBR console.
2. In the left-side navigation pane, choose On-Premises Backup > VM Client.
3. In the upper-right corner of the page, click Create Client.
4. In the Create Client dialog box, configure the required settings and click Create. Settings are described as follows.

Name	Description
Backup Vault Name	A backup vault is an HBR cloud warehouse used to store backup data on the cloud. Backup data from multiple clients can be stored in the same vault. · One or more backup vaults available You can select a backup vault on the drop-down list . · No backup vault available Click Create Vault. Enter the Backup Vault Name and Vault Description to create a new backup vault. The vault name must be a maximum of 32 characters in length.
Client Name	The name of the backup client. The client name must be a maximum of 32 characters in length.
Software Platform	vSphere is selected by default.
Network Type	· Virtual Private Cloud (VPC): Select this option when the virtual machine to be backed up is located in a VPC and in the same region where the backup vault is located. · Public Network: Select this option when VPCs are not applicable.

5. Click Download Client and Download Certificate.

 Note:

You can install a client to connect a virtual machine to Hybrid Backup Recovery (HBR) and use the certificate to activate the client. You can also go to the File Client page and download a client at any time.

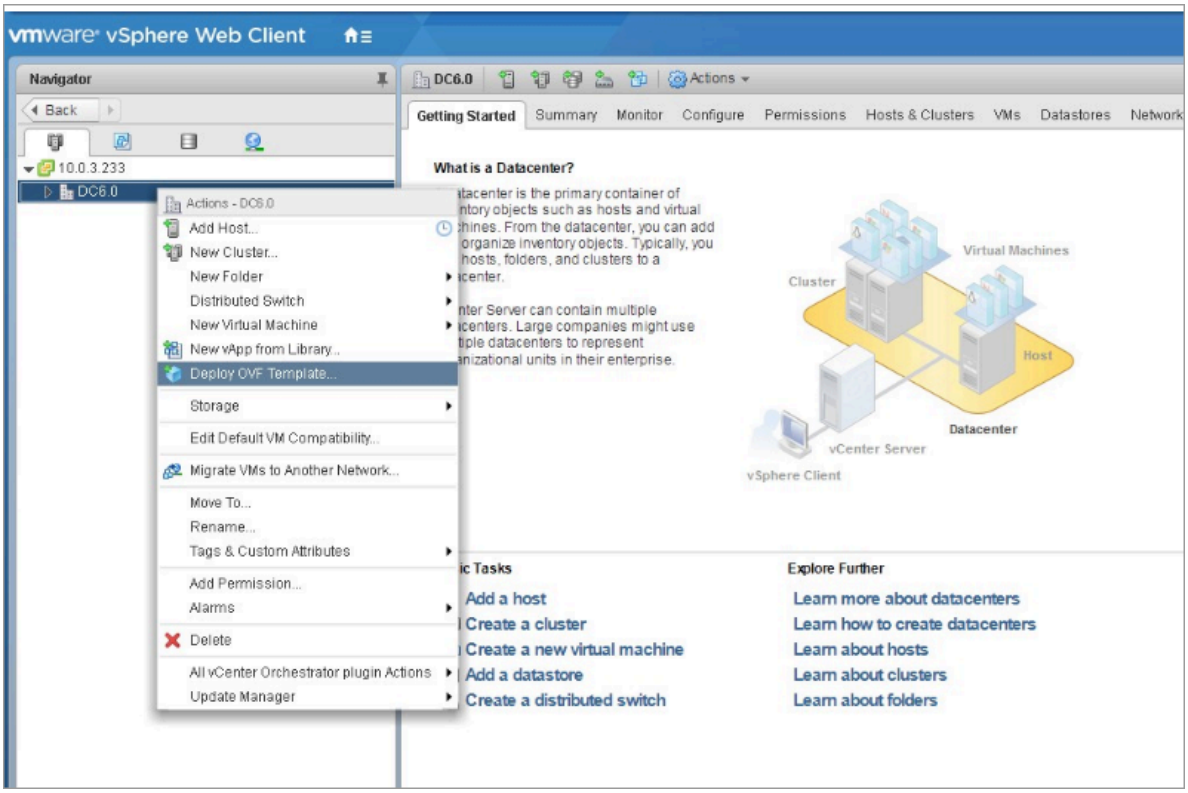
Install a client

After downloading a client and certificate, you need to install the client. After the client is installed, you can use the client to perform backup and restore jobs. You can perform the following steps to install a client:

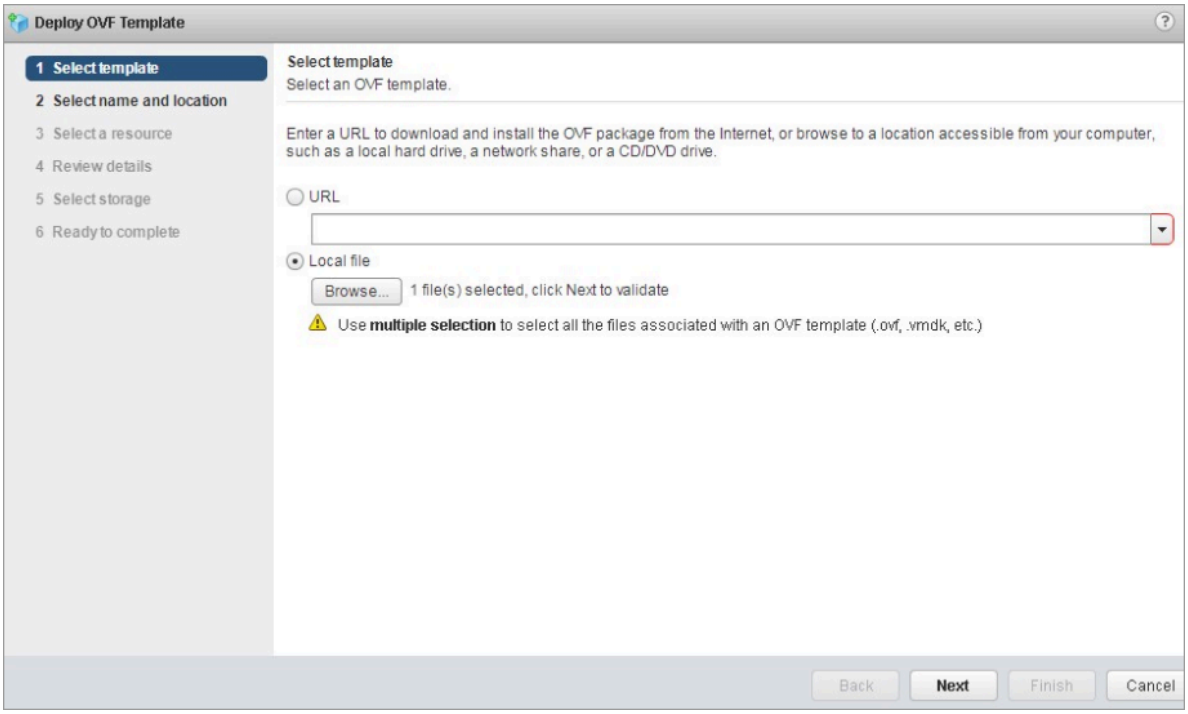
1. Log on to the vSphere Web Client.

   Note:
   HBR only supports vCenter Server 5.5, 6.0, and 6.5.

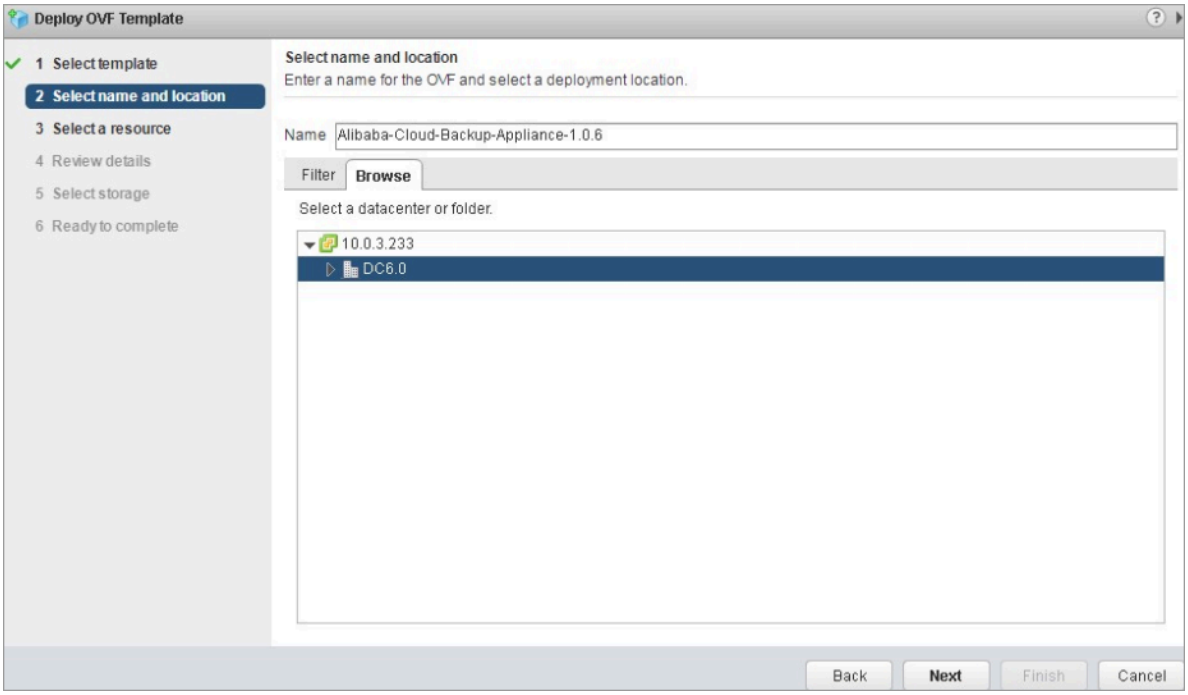
2. In the left-side navigation pane, right-click the virtual machine that you need to deploy an OVF template and select Deploy OVF Template.



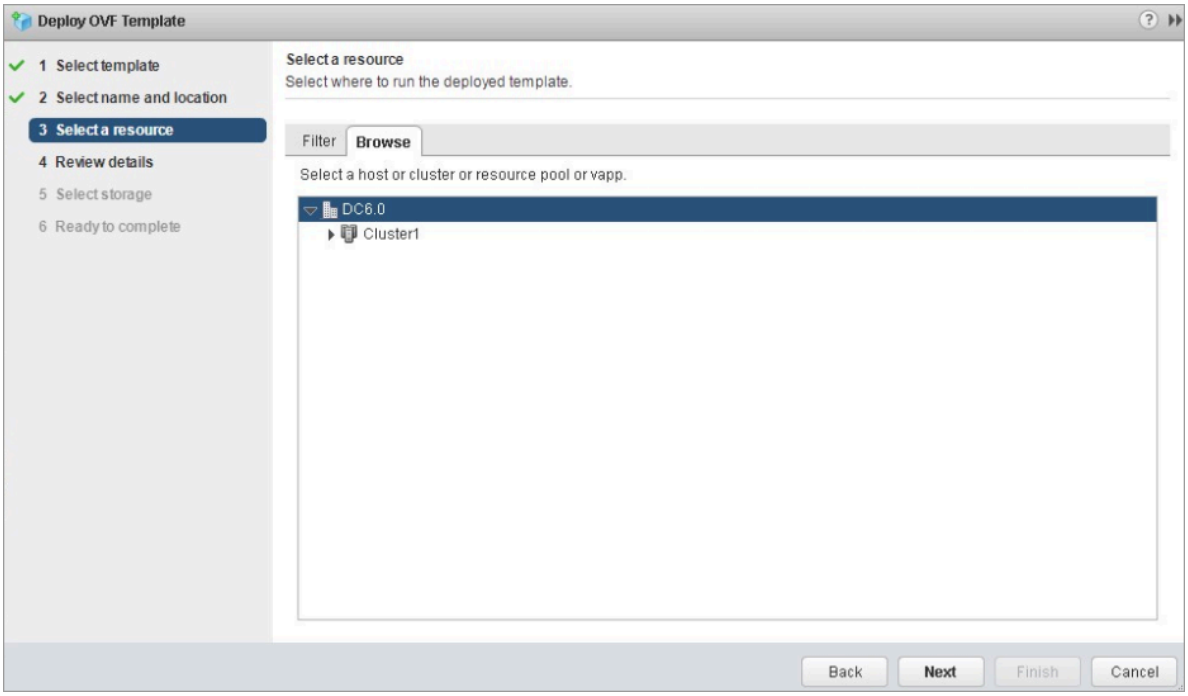
3. In the Deploy OVF Template dialog box, select Local File. Click Browse to select a downloaded client file, and then click Next.



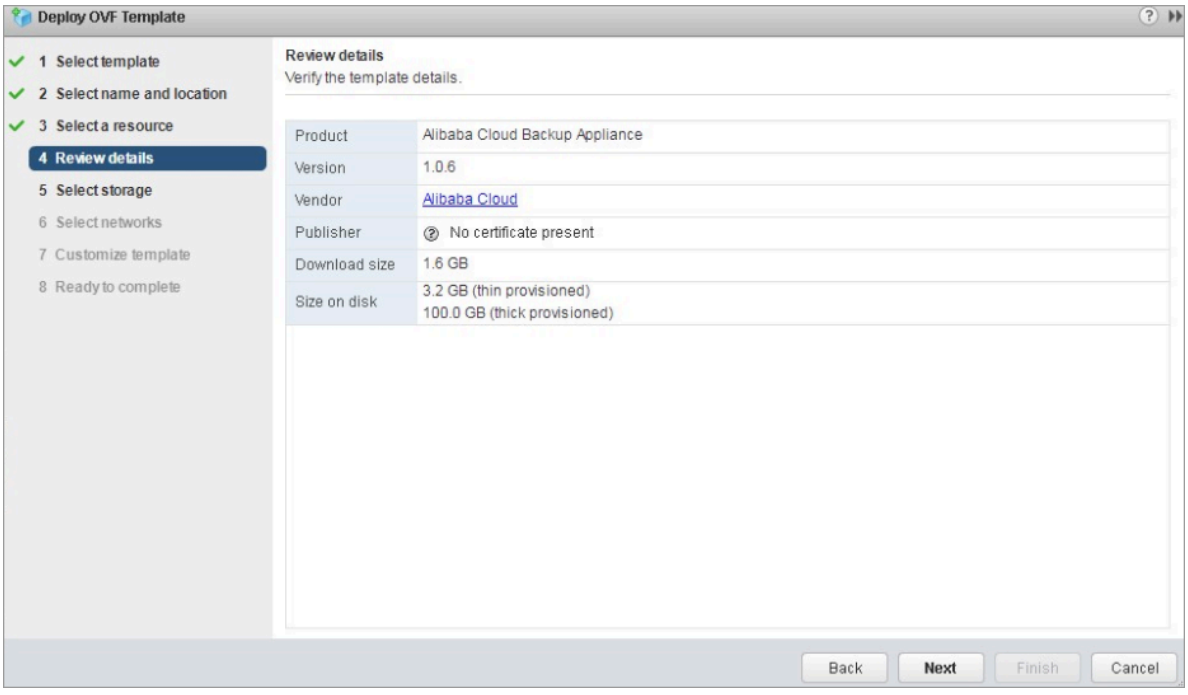
4. Enter the name of the OVF template, select a location you need to deploy the OVF template, and then click Next.



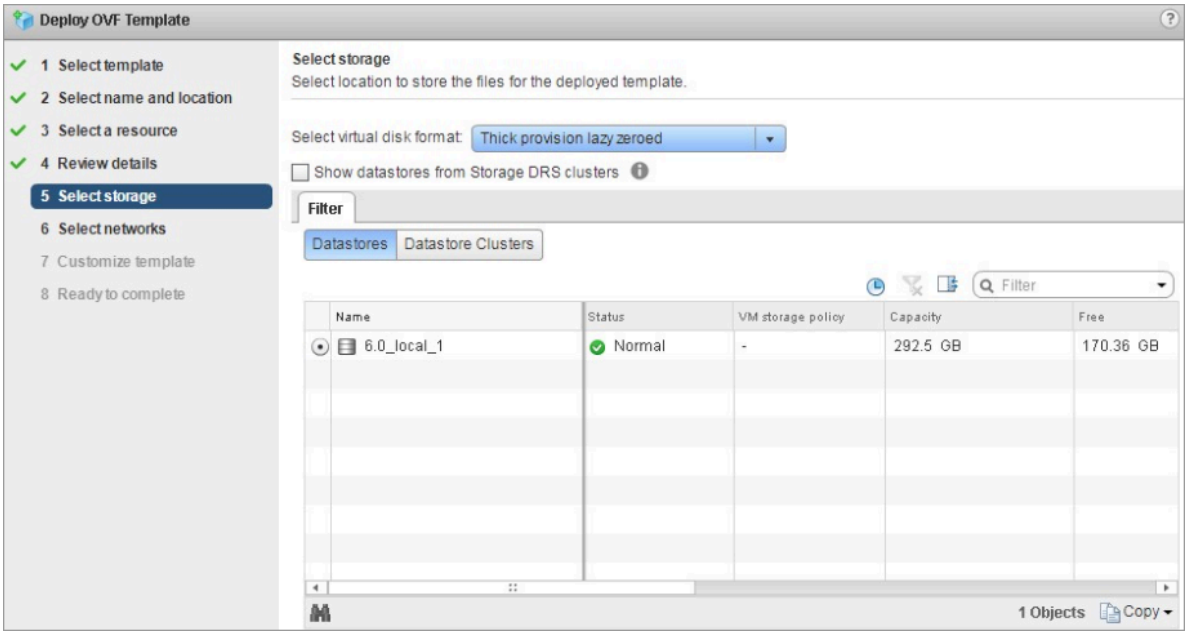
5. Select a location where you need to run the deployed template, and then click Next.



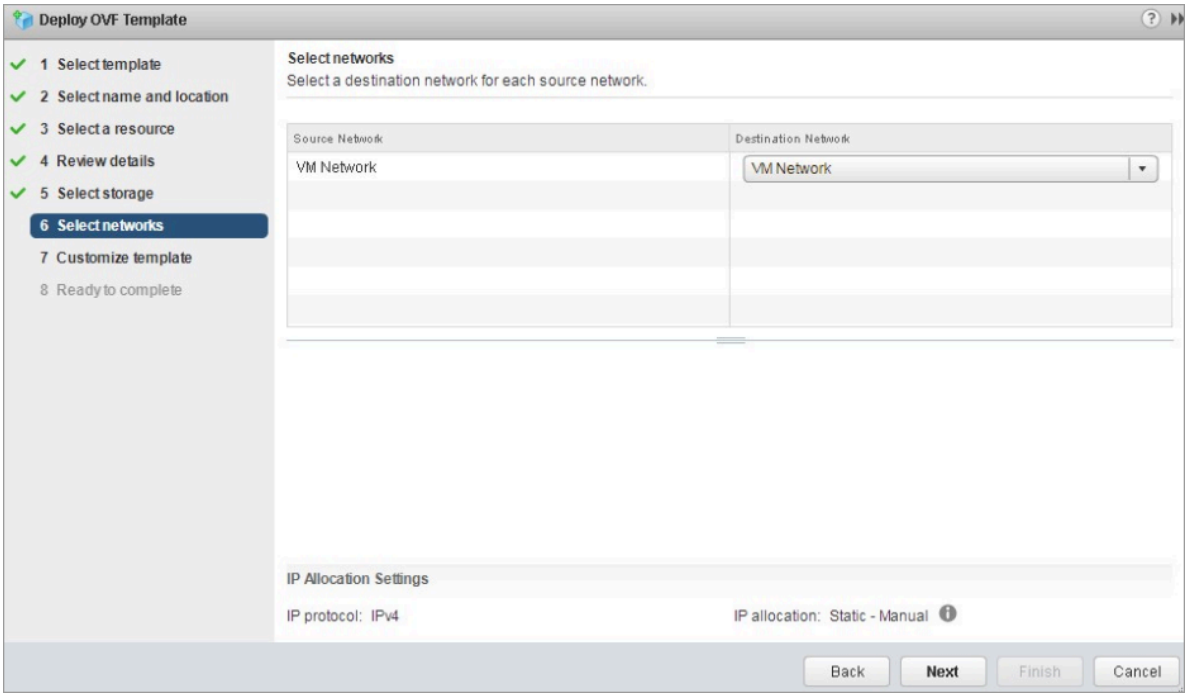
6. Verify the details of the template, and click Next.



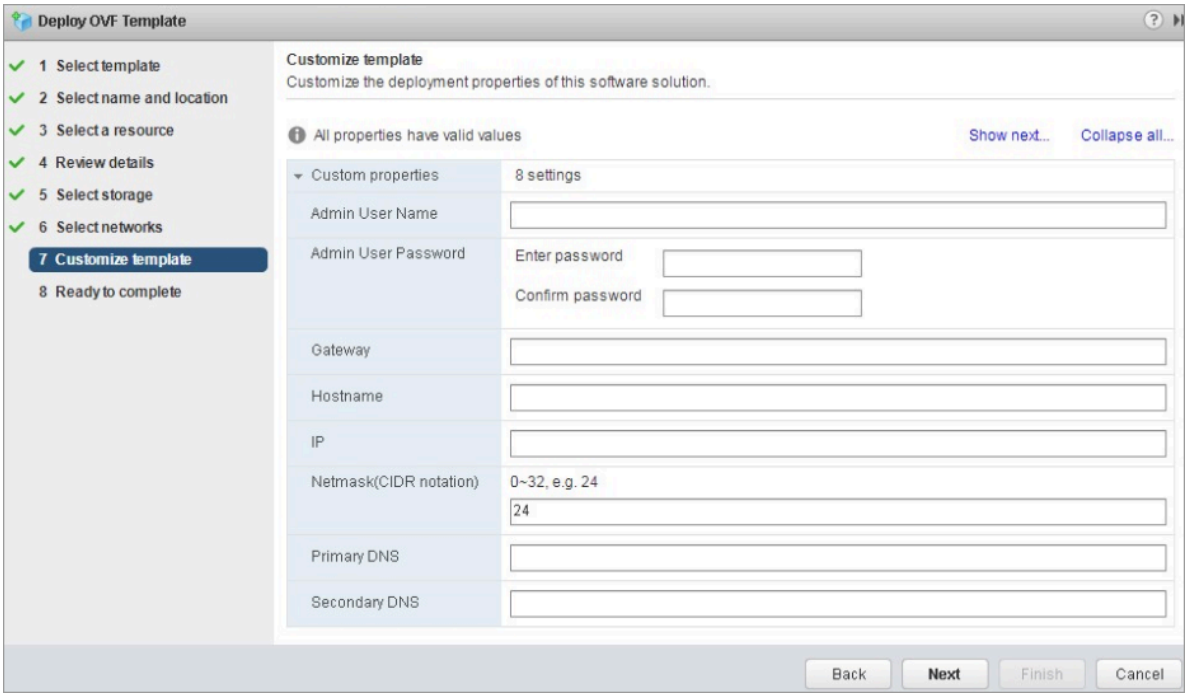
7. Select the required virtual disk format, select a datastore to store the deployed OVF template, and then click Next.



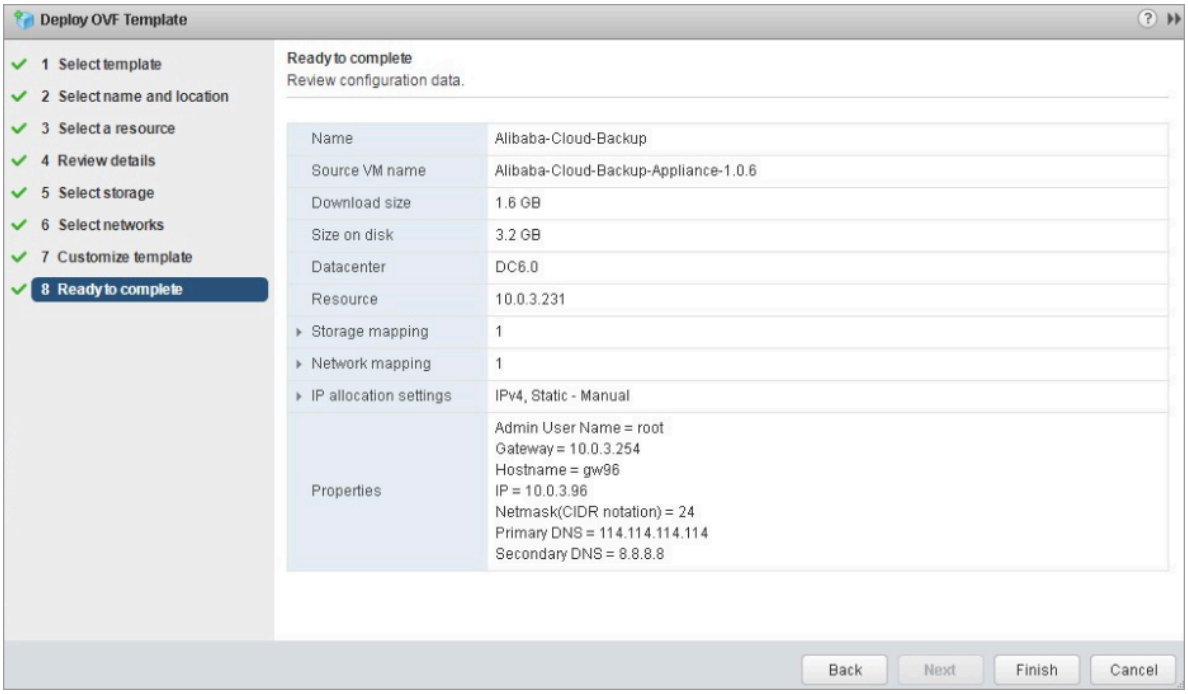
8. Select a source network, map the network to a destination network, and click Next.



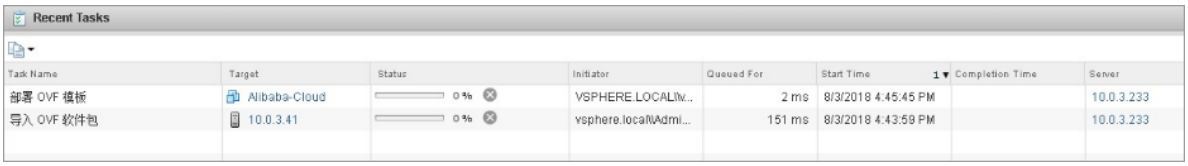
9. Customize the deployment properties for the software solution, and click Next.



10. View the configuration details, and click Finish.



11. On the `Recent Tasks` page, you can view the progress of the deployment task. This process may take a few minutes.



12. After the OVF template is deployed, turn on the virtual machine that is deployed by using the OVF template.
13. Open a browser and enter `https :// hostname : 8443` in the address bar.

> Note:
> The `hostname` is the IP address of the virtual machine that is deployed by using the OVF template.

14. In the Activate Gateway dialog box, configure the required settings and click Register to log on to the Hybrid Backup Gateway console. Settings are described in the following table.

Name	Description
AccessKey ID and AccessKey Secret	Download the AccessKey ID and AccessKey Secret of the Alibaba Cloud account where the Hybrid Backup Recovery (HBR) service is activated.
Password	The logon password of the client. The password must be a minimum of six characters in length.
Certificate	The certificate you have downloaded from the HBR console. The validity period of each certificate is two days. You must download a new certificate to register a client when the certificate in use expires.

(Optional) Create a backup plan and backup policy

Before you perform a backup job, we recommend that you schedule the backup time and interval of the backup job based on the business requirements.

- If no regular backup plan exists, you can skip this step.
- If you have a regular backup plan, you can perform the following steps to create a backup policy and specify the first backup time and backup interval. Proceed as follows:

1. Log on to the Hybrid Backup Gateway console, in the top navigation pane, select Backup Policies, and click Create Backup Policy.

2. Enter the Policy Name, and specify the Effective Time and Backup Interval. For example, if you set the backup interval to one day, a backup job is run at the specified time every day.
3. Click Submit.

2.3 Back up the image of a VMware virtual machine

You can use a VM client to back up the image of a local virtual machine. HBR supports the following backup modes: instant backup and scheduled backup. You can select the required backup mode based on your business needs.

Instant backup

If you have no regular backup plan and only need to perform a full backup, you can perform the following steps:

1. Log on to the Hybrid Backup Recovery Gateway. In the top navigation pane, select Backup.
2. Add target backup servers. Click Add Server in the upper-right corner or choose Actions > Add Server.
3. In the Add Server dialog box, enter the `Type`, `IP Address`, `Username`, and `Password`, and click OK.
4. In the upper-right corner of the page, click Create Backup Plan.
5. Enter the `Plan Name`, specify the `Retention`, and select Instant. Click Next.
6. Select one or more virtual machines and click Next.
7. Confirm the backup and virtual machine information, and click Create.

Note:

After a backup plan is created, you can view the details of the backup plan on the `Backup Plans` tab.

Scheduled backup

If you have a regular backup plan, you can create a scheduled backup based on a custom backup policy. Proceed as follows:

1. Log on to the Hybrid Backup Recovery Gateway. In the top navigation bar, click Backup.

2. Click Add Server in the upper-right corner or choose Actions > Add Server to add the target backup server.
3. In the Add Server dialog box, enter the IP address, username, and password of the target backup server, and click OK.
4. Click Create Backup Plan.
5. Enter the name of a backup plan, select a retention period, and select Scheduled.
6. Select a full backup policy. If you need to perform an incremental backup, select an incremental backup policy and click Next.

   Note:
   When you perform an incremental backup for a virtual machine, you must enable Changed Block Tracking (CBT) on the virtual machine. For more information about CBT, see VMware documentation.
7. Select one or more virtual machines, and then click Next.
8. Confirm the backup and virtual machine information, and click Create.

   Note:
   After a backup plan is created, you can view the details of the backup plan on the `Backup Plans` tab.

2.4 Restore a backup image to the source VMware virtual machine

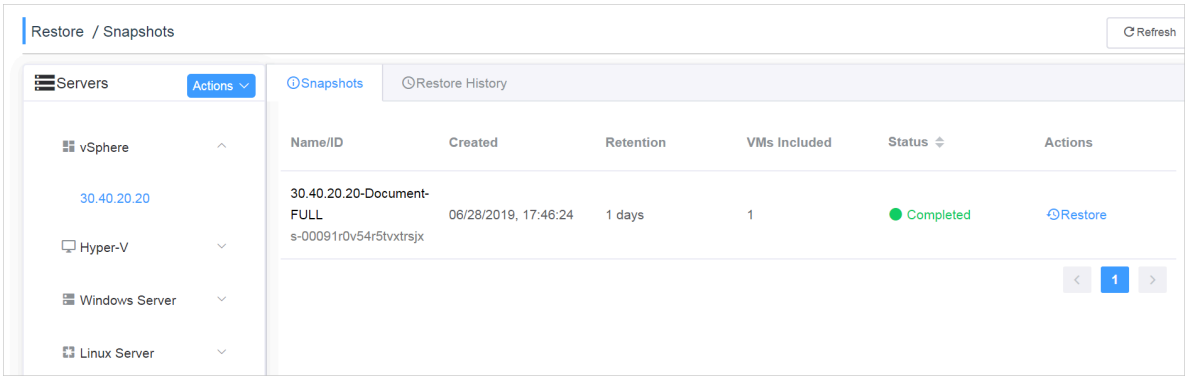
This topic describes how to restore a backup image to the source virtual machine.

Procedure

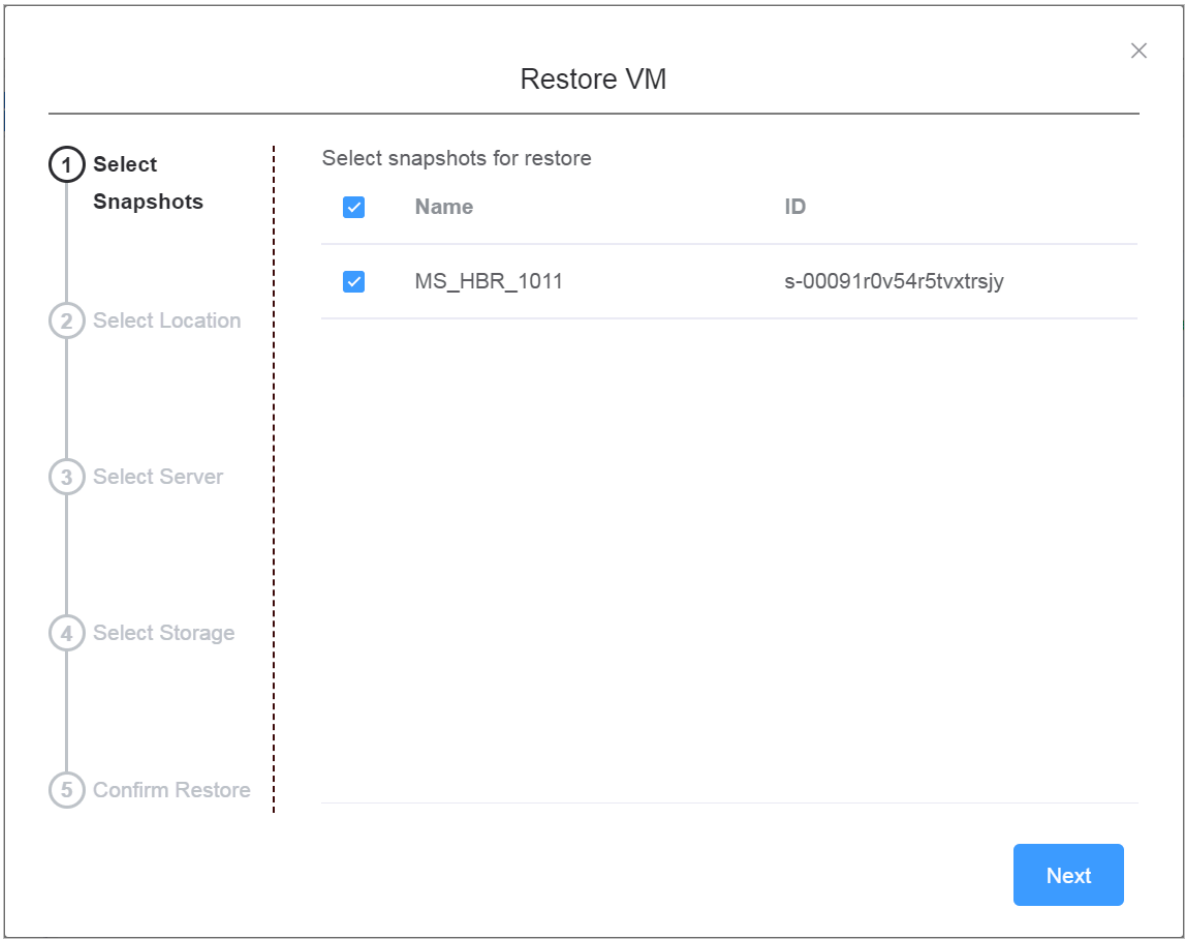
1. Open a browser and enter `https :// hostname : 8443` in the address bar.

   Note:
   The `hostname` is the IP address of the source virtual machine.
2. In the top navigation pane, select Restore.

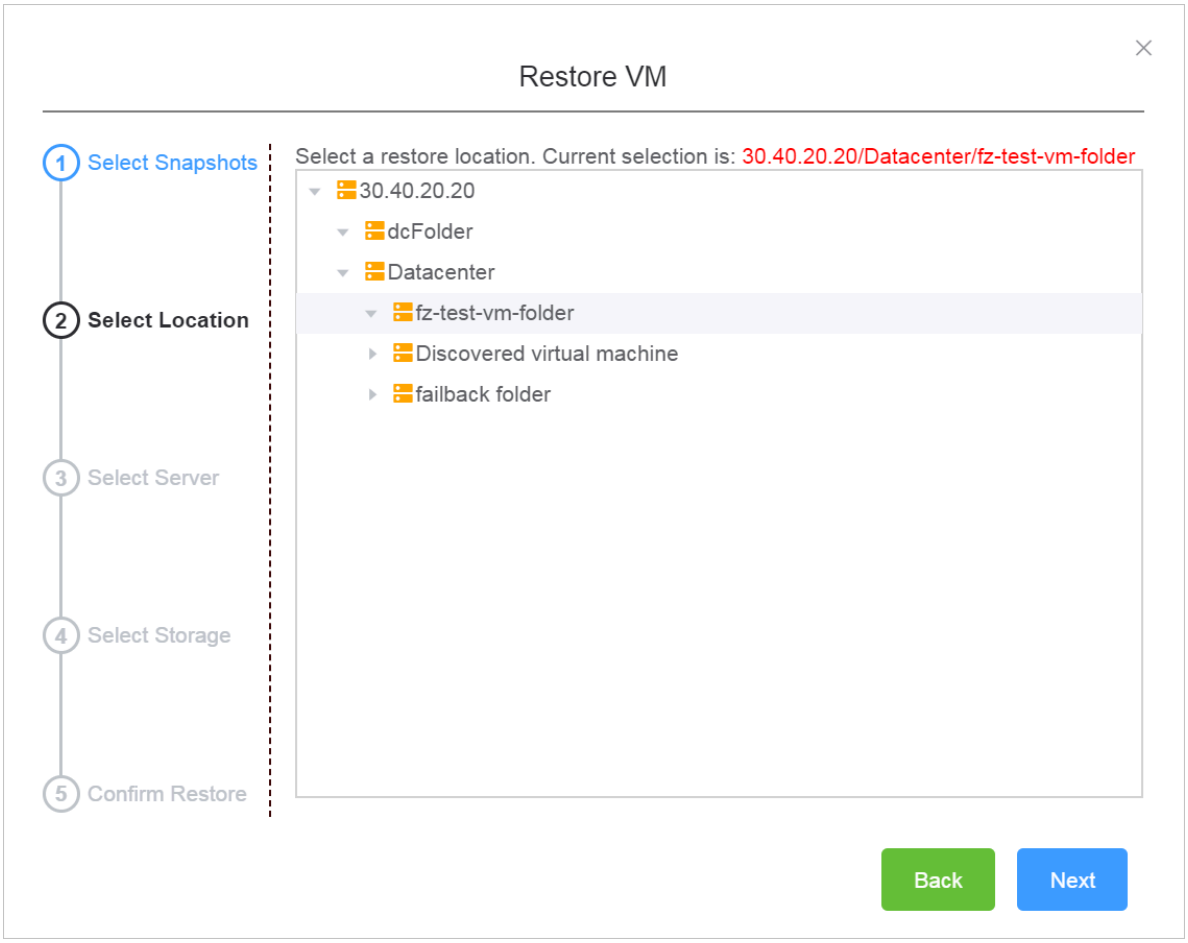
3. In the left-side navigation pane, select a server. On the Snapshots tab, select a snapshot and click Restore.



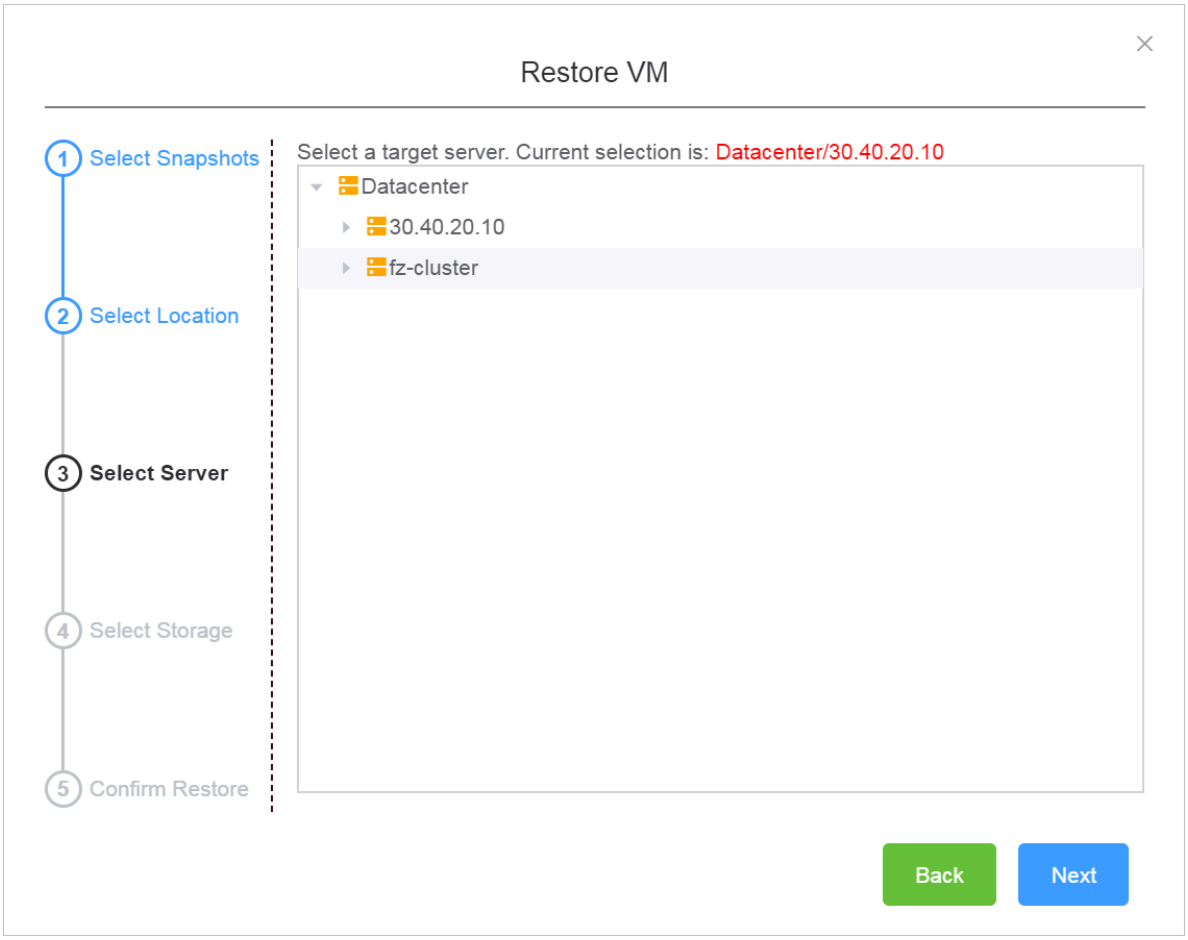
4. In the Restore VM dialog box, select the required snapshot and click Next.



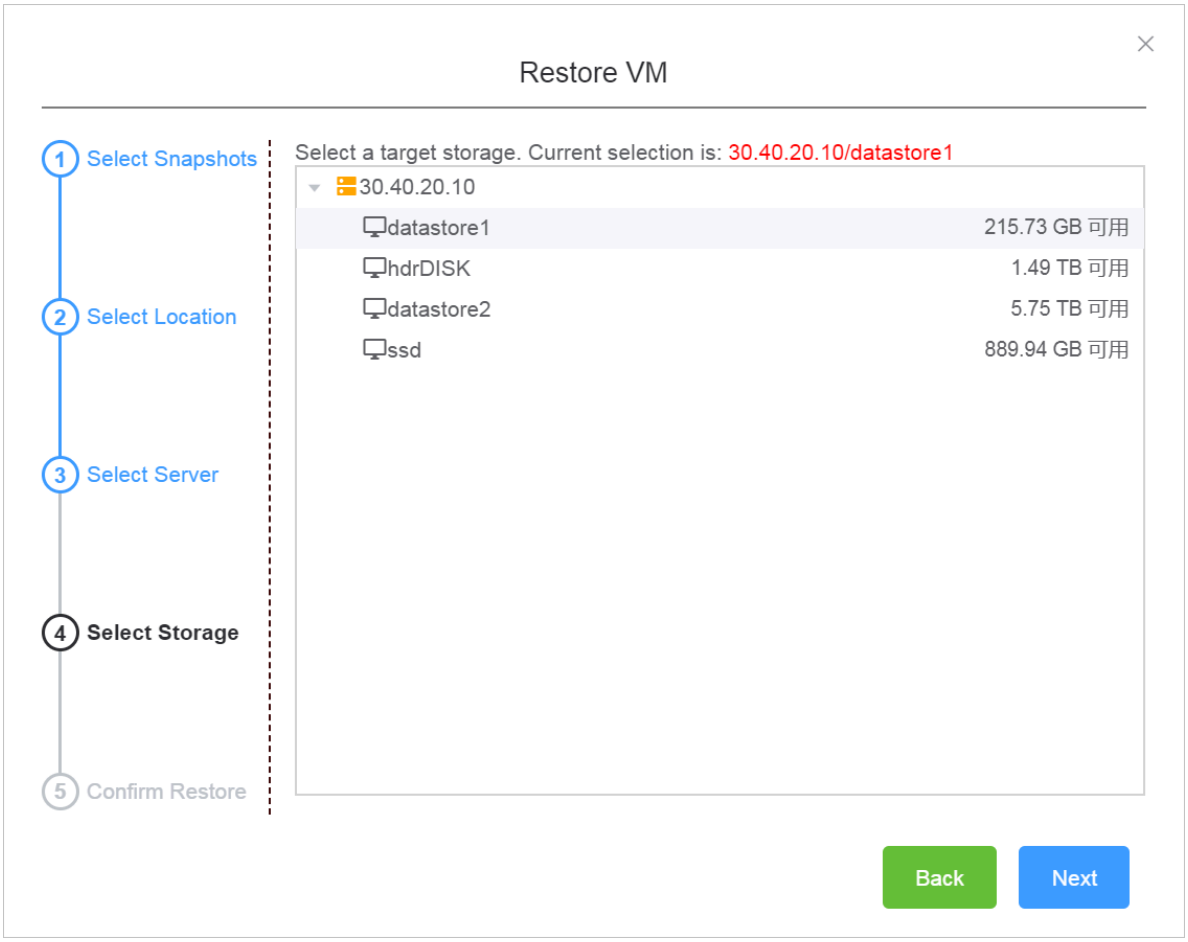
5. **Select the required location and click Next.**



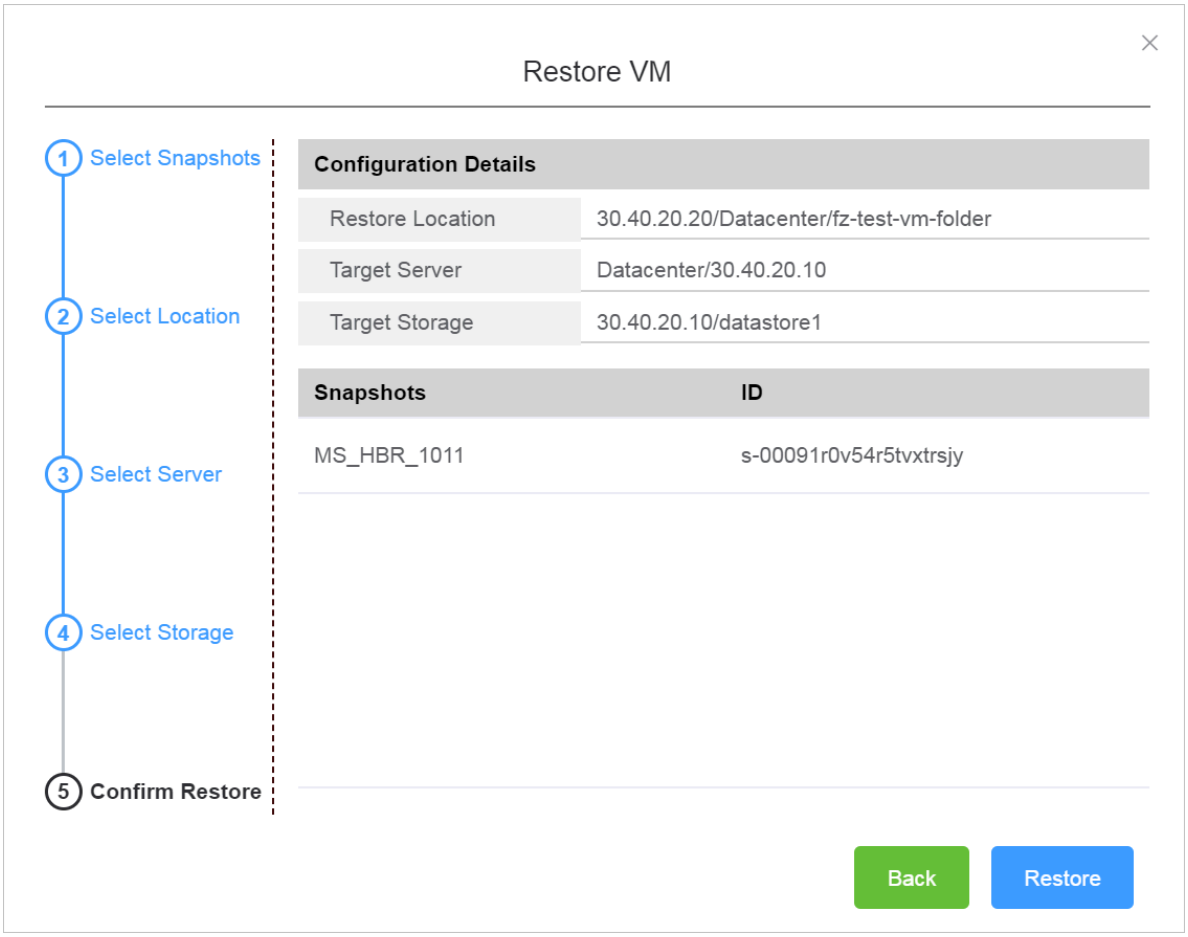
6. **Select the target server and click Next.**



7. **Select the target drive and click Next.**



8. Confirm the restore information and click Restore.



9. Select the `Restore History` tab and view the details of a restore job, such as the status, target location, and amount of restored data.

2.5 Backup alerts

Backup alerts provide you with backup 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, or 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

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

1. Log on to the Hybrid Backup Recovery console.

2. In the left-side navigation pane, select Alarm Contact.
3. Select the Alarm Contact tab.
4. In the upper-right corner, click New Contact.
5. In the New Contact dialog box, enter the Contact Name .
6. Select the required Contact Method and perform the following actions:
   - Email

     If you select Email as a contact method, enter the Contact Email and then click Send Verification. Log on to the specified mailbox to view the verification code, go 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 click Send Verification. An SMS message that contains a verification code will be sent to your mobile phone. Enter the verification code in the Mobile Verificati on Code field.
7. Click OK.

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

Create an alarm contact group

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

1. Log on to the HBR console.
2. In the left-side navigation pane, select Alarm Contact.
3. 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 that you need to add to the group, and click the  icon. These contacts are displayed in the `Selected Contacts` field.
7. Click OK.

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

Create custom alarm policies

You can create the following types of alarm policies:

- Vault-level alarm policies

  A vault-level alarm policy applies to all the backup clients of a vault. The backup clients include those installed on ECS instances, local hosts, and local virtual machines. If you create an alarm policy for a vault where the client is located but not for a client, the alarm policy of the vault applies to the client by default.
- Instance-level alarm policies

  An instance-level alarm policy applies to the backup client installed on a specific instance. After you create an alarm policy for a client, the client no longer uses the alarm policy of the vault or the default alarm policy.

> Note:
> If you do not create an alarm policy for a vault or a client, alerts are sent to an Alibaba Cloud account by using emails.

Create a vault-level alarm policy

Proceed as follows:

1. Log on to the HBR console.
2. On the Overview page, locate the required vault to create an alarm policy.
3. In the upper-right corner of a vault, click Settings.

4. In the Vault Setting dialog box, select the required `Alarm Policy`.
   - Disabled

     If you select this option, no alert is sent when an alarm occurs on a client or ECS instance that is located in the vault.
   - Default Notification

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

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

Create an instance-level alarm policy

Proceed as follows:

1. Log on to the HBR console.
2. Locate a client for which you need to create an alarm policy, choose More > Alarm Setting next to the client.
3. In the Alarm Policy dialog box, select the required `Alarm Policy`.

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

4. Click OK.

3 Workflow-based backup

3.1 Overview

You can use Hybrid Backup Recovery (HBR) to back up workflow-based data sources and restore backups as needed.

You can use a file client to back up data sources that are located in a local data center. These data sources include SAP HANA, SQL Server, MySQL, and MongoDB.

- Prerequisites
- Back up data from SAP HANA / Back up data from SQL Server / Back up data from MySQL / Back up data from MongoDB
- Restore a backup

The following functions are related to this topic:

- Search backups
- Mirror vaults

3.2 Prerequisites

Hybrid Backup Recovery (HBR) allows you to backup data from workflow-based data sources. Supported data sources include SAP HANA, SQL Server, Oracle, MySQL, MongoDB, and Hyper-V. The following prerequisites are required before you perform a backup job.

RAM users and AccessKeys

Resource Access Management (RAM) enables you to manage user access to Alibaba Cloud resources. You can create and manage multiple RAM users with a single Alibaba Cloud account. You can grant different permissions for each RAM user. This allows each RAM user to have different permissions to access Alibaba Cloud resources.

An AccessKey is required when you activate a backup client. As any leak of an Alibaba Cloud account's AccessKey will expose cloud resources to security risks, we recommend that you use the AccessKey of a RAM user to perform the activation.

Before performing a backup job, ensure that you have Created a RAM user and Created an access key for a RAM user.

Download a client

You can use HBR backup clients to perform backup and restore jobs. You can perform the following steps to download a backup client to a server or virtual machine to be backed up.

1. In the left-side navigation pane, choose On-Premises Backup > File Client.
2. In the upper-right corner, click Create Client.
3. In the Create Client dialog box, configure the required settings and click Create. Settings are described in the following table.

Name	Description
Backup Vault Name	A backup vault is an HBR cloud warehouse used to store backup data on the cloud. Backup data from multiple clients can be stored in the same vault. · One or more backup vaults available You can select a backup vault on the drop-down list. · No backup vault available Click Create Vault. Enter the Backup Vault Name and Vault Description to create a new backup vault. The vault name must be a maximum of 64 characters in length.
Client Name	The name of the backup client. The client name must be a maximum of 64 characters in length.
Software Platform	The operating system that is running on a host from which you need to back up data. Valid values: · Windows 32-bit · Windows 64-bit · Linux 32-bit · Linux 64-bit
Network Type	· Virtual Private Cloud (VPC): Select this option when the host to be backed up is located in a VPC and in the same region where the backup vault is located. · Public Network: Select this option when VPCs are not applicable.

4. Click Download Client.

> Note:
> You can install a client to connect a host to Hybrid Backup Recovery (HBR). You can also go to the File Client page and download a client at any time.

Install and activate a client

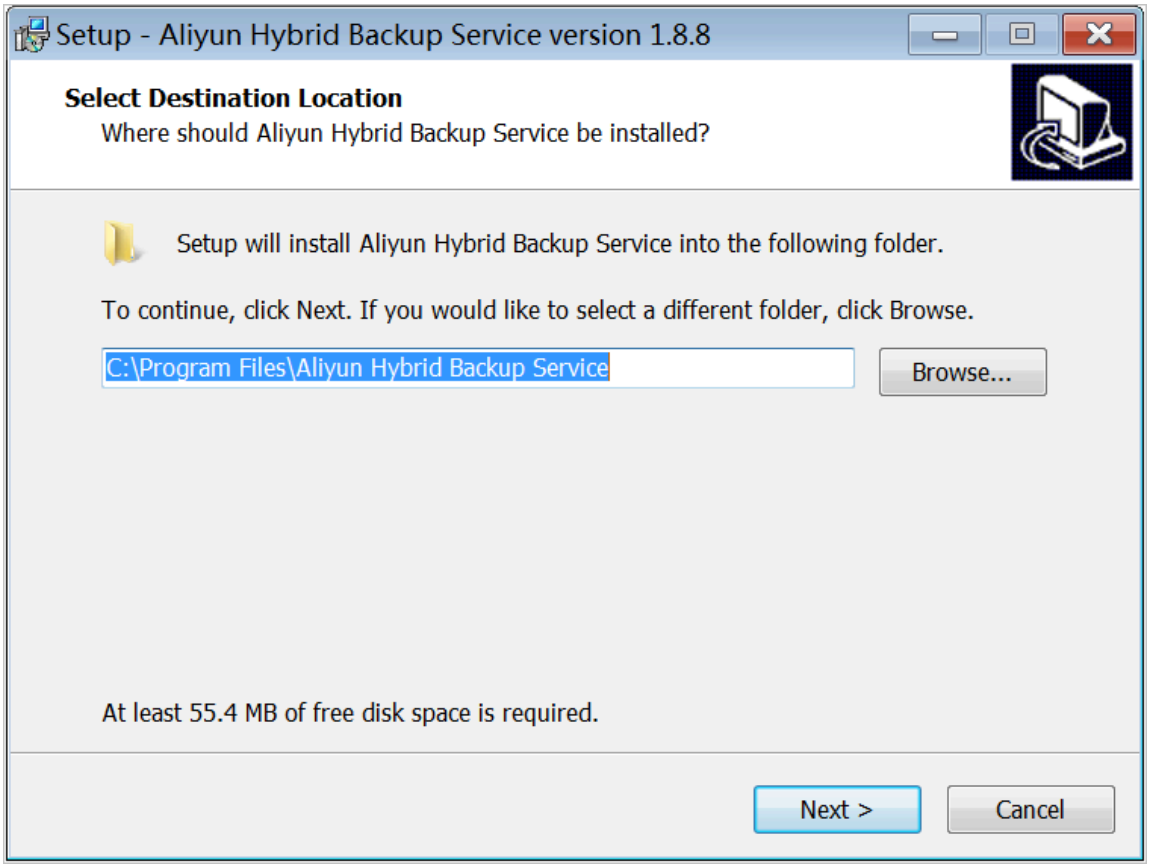
After downloading a client and certificate to a server or virtual machine from which you need to back up data, you need to install the client. Proceed as follows:

1. Install a client from an installation package and select an installation folder.

> Note:

As operation logs and an executable file are all stored in the installation folder, you must ensure that enough space is available.

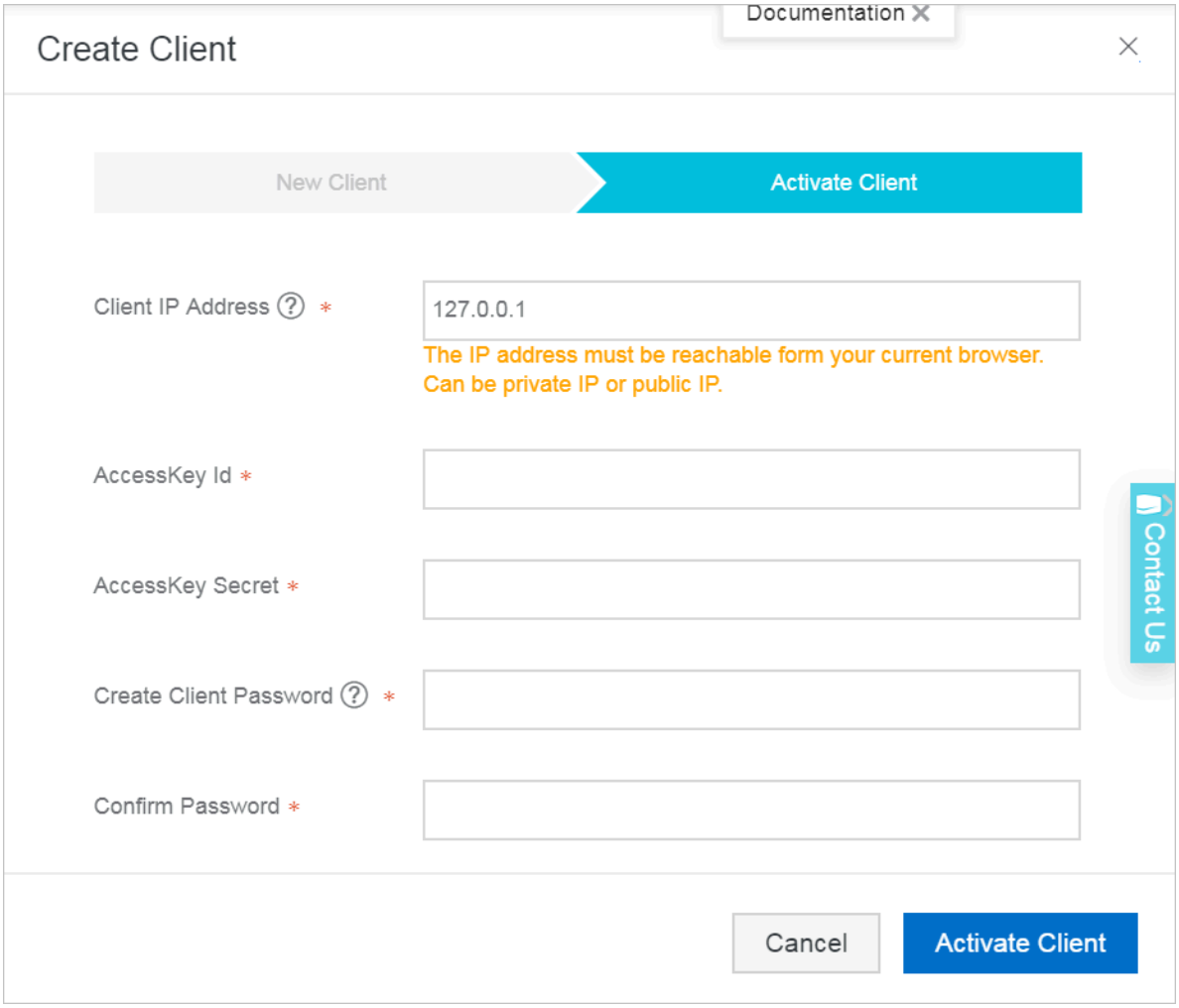
- If you install a client on Windows, run an installation package, select an installation folder, and follow the instructions to complete the installation.



- If you install a client on Linux, extract an installation package to a folder and run the `./ setup` command to install the client.

```
[root@47 software]# tar -zxvf hbr-install-1.3.4-linux-amd64.tar.gz
hbr-install-1.3.4-linux-amd64/
hbr-install-1.3.4-linux-amd64/client/
hbr-install-1.3.4-linux-amd64/download/
hbr-install-1.3.4-linux-amd64/logs/
hbr-install-1.3.4-linux-amd64/setup
hbr-install-1.3.4-linux-amd64/uninstall
hbr-install-1.3.4-linux-amd64/update/
hbr-install-1.3.4-linux-amd64/versions/
hbr-install-1.3.4-linux-amd64/update/updater
hbr-install-1.3.4-linux-amd64/client/hybridbackup
hbr-install-1.3.4-linux-amd64/client/ids
hbr-install-1.3.4-linux-amd64/client/resource/
hbr-install-1.3.4-linux-amd64/client/www/
hbr-install-1.3.4-linux-amd64/client/www/dist/
hbr-install-1.3.4-linux-amd64/client/www/dist/index.html
hbr-install-1.3.4-linux-amd64/client/www/dist/static/
hbr-install-1.3.4-linux-amd64/client/www/dist/static/css/
hbr-install-1.3.4-linux-amd64/client/www/dist/static/fonts/
hbr-install-1.3.4-linux-amd64/client/www/dist/static/img/
hbr-install-1.3.4-linux-amd64/client/www/dist/static/js/
hbr-install-1.3.4-linux-amd64/client/www/dist/static/js/app.7e558a4017f7c8ad58a4.js
hbr-install-1.3.4-linux-amd64/client/www/dist/static/js/manifest.afb9fdc23e85cda133f8.js
hbr-install-1.3.4-linux-amd64/client/www/dist/static/js/vendor.cbd4977a3094b35cf5a3.js
hbr-install-1.3.4-linux-amd64/client/www/dist/static/img/hbr_logo.b8bbcfb.png
hbr-install-1.3.4-linux-amd64/client/www/dist/static/img/logo.1922e1b.png
hbr-install-1.3.4-linux-amd64/client/www/dist/static/img/logotxt.827883a.png
hbr-install-1.3.4-linux-amd64/client/www/dist/static/img/logotxt_en.eefd9c8.png
hbr-install-1.3.4-linux-amd64/client/www/dist/static/fonts/element-icons.6f0a763.ttf
hbr-install-1.3.4-linux-amd64/client/www/dist/static/fonts/iconfont.012cf6a.woff
hbr-install-1.3.4-linux-amd64/client/www/dist/static/fonts/iconfont.a24068e.woff2
hbr-install-1.3.4-linux-amd64/client/www/dist/static/fonts/iconfont.a37b0c0.ttf
hbr-install-1.3.4-linux-amd64/client/www/dist/static/css/app.2af72af1fc9bac8fc91108877b2708bc.css
hbr-install-1.3.4-linux-amd64/client/resource/en-US.json
hbr-install-1.3.4-linux-amd64/client/resource/zh-CN.json
[root@47 software]# cd hbr-install-1.3.4-linux-amd64
[root@47 hbr-install-1.3.4-linux-amd64]# ll
total 28
drwxr-xr-x 4 501 games 4096 Sep 21 16:31 client
drwxr-xr-x 2 501 games 4096 Sep 12 10:36 download
drwxr-xr-x 2 501 games 4096 Sep 12 10:36 logs
-rwxr-xr-x 1 501 games  307 Sep 12 10:36 setup
-rwxr-xr-x 1 501 games  233 Sep 12 10:36 uninstall
drwxr-xr-x 2 501 games 4096 Sep 21 16:31 update
drwxr-xr-x 2 501 games 4096 Sep 12 10:36 versions
[root@47 hbr-install-1.3.4-linux-amd64]# ./setup
Setting up Hybrid backup client ...
Complete
[root@47 hbr-install-1.3.4-linux-amd64]#
```

2. After a client is installed, you need to activate the client. Go to the HBR console. In the Create Client dialog box, click Next, and configure the required settings as described in the following table to activate the client.



Note:
We recommend that you download and install a client before activating the client.

Name	Description
Client IP address	The IP address of the file client. The host you are working with must be able to access the IP address of the file client. The IP address is either an internal IP address or public IP address. For example, 127.0.0.1 (default), 12.34.56.78:8011, and http://87.65.43.21:8443. **Note:** The IP address must be accessible by a browser.

Name	Description
AccessKey ID	Download the AccessKey ID and AccessKey Secret of the Alibaba Cloud account where the HBR service is activated.
AccessKey Secret	Download the AccessKey ID and AccessKey Secret of the Alibaba Cloud account where the HBR service is activated.
Create Client Password	Set the logon password of the client. The password must be a minimum of six characters in length.

3. Click Activate Client to open a web page. You can use this web page to manage the file client. You can use a file client to back up data.

If you fail to activate a client, you can use one of the following methods to reactivate the client:

- Reactivate a client in the console

  Go to the File Client page, and click Activate Client in the `Actions` column of a failed client to reactivate the client.
- Reactivate a client on a web page

  Go to the File Client page and click Download Certificate in the `Actions` column. Open a browser and enter `http :// localhost : 8011` in the address bar to open the Initialize Register page. Configure the required settings as described in the following table and click Register to activate the client.

Name	Description
Upload Certificate	You can upload the token you have downloaded from the console. The token is used as a certificate. The validity period of each certificate is two days. You must download a new certificate to register a client when the certificate in use expires.
AccessKey ID and AccessKey Secret	Download the AccessKey ID and AccessKey Secret of the Alibaba Cloud account where the HBR service is activated.
Network Type	- Virtual Private Cloud (VPC): Select this option when the host to be backed up is located in a VPC and in the same region where the backup vault is located. - Classic Network: Select this option when VPCs are not applicable.
Password	Set the logon password of the client. The password must be a maximum of six characters in length.

Name	Description
Encrypt AccessKey	If you use the password to encrypt the AccessKey, you must enter the password after each restart.

If you perform a backup operation on an intermediate host, you must change `localhost` to the IP address of the server or virtual machine from which you back up data.

Port 8011 is the default port that you can use to logon to a file client. If port 8011 on the server or virtual machine is occupied by another application, you can specify another port number for the file client.

(Optional) Create a backup plan and backup policy

Before you perform a backup job, we recommend that you schedule the backup time and interval of the backup job based on your business requirements.

- If no regular backup plan exists, you can skip this step.
- If you have a regular backup plan, you can perform the following steps to create a backup policy and specify the first backup time and backup interval.

Proceed as follows:

1. Open a browser and enter `http :// localhost : 8011` in the address bar and enter the password to log on to an HBR file client.

   Note:

   - If you perform a backup operation on an intermediate host, you must change `localhost` to the IP address of the server or virtual machine from which you need to back up data.
   - Port 8011 is the default port that you can use to logon to a file client. If port 8011 on the server or virtual machine is occupied by another application, you can specify another port number for the file client.
2. In the left-side navigation pane, select Backup Policies.
3. On the Backup Polices page, click Create Policy.

4. In the Create Policy dialog box, enter the `Name` , configure the required settings as described in the following table, and click Submit.

Name	Description
Name	The name of the backup policy.
Frequency	Unit: · Hour. Valid values: 1 to 23. · Day. Valid values: 1 to 6. · Week. Valid values: 1 to 4.
Backup Time	The first backup time. The first backup is a full backup.
Retention	· Unit: day, month, and year. · Maximum retention period: 3650 days (10 years).

Note:

If you need to delete or modify a backup policy, locate the required backup policy, click Delete or Edit next to the backup policy. After a backup policy is deleted, you cannot run the backup job to which the backup policy applies. The backups that correspond to the backup job are also deleted.

More operations

Back up data from SAP HANA

Back up data from SQL Server

Back up data from MySQL

Back up data from MongoDB

3.3 Back up SAP HANA

This topic describes how to use Hybrid Backup Recovery (HBR) to back up data from on-premises SAP HANA.

Notice:

Before the backup, you must disable the backup policy of SAP HANA.

Prerequisites

You have completed the preparations.

Step 1: Create a file named workflow.env

1. Go to the installation directory of the HBR backup client and create a file named `workflow.env` in the `client` subdirectory.

   > **Note:**
   > The `workflow.env` file must be stored in the same directory as the `hybridebackup` and `ids` executable files.

2. In the `workflow.env` file, enter the username and password of a backup source in the following format:

```
USERNAME = root
PASSWORD =****
```

Step 2: Configure backup scripts

Pre-backup script

1. Download the pre-backup script for SAP HANA.
2. Configure and save the pre-backup script. The following section describes the parameters that need to be configured in the pre-backup script for SAP HANA. You can configure these parameters as required.

Parameter	Description
HDB_SQL=/usr/sap/<SID>/HDB01/exe/hdbsql	The path of the SQL client for SAP HANA.
INSTANCE_ID	The ID of the database.
HANA_HOST	The host name of the master node.

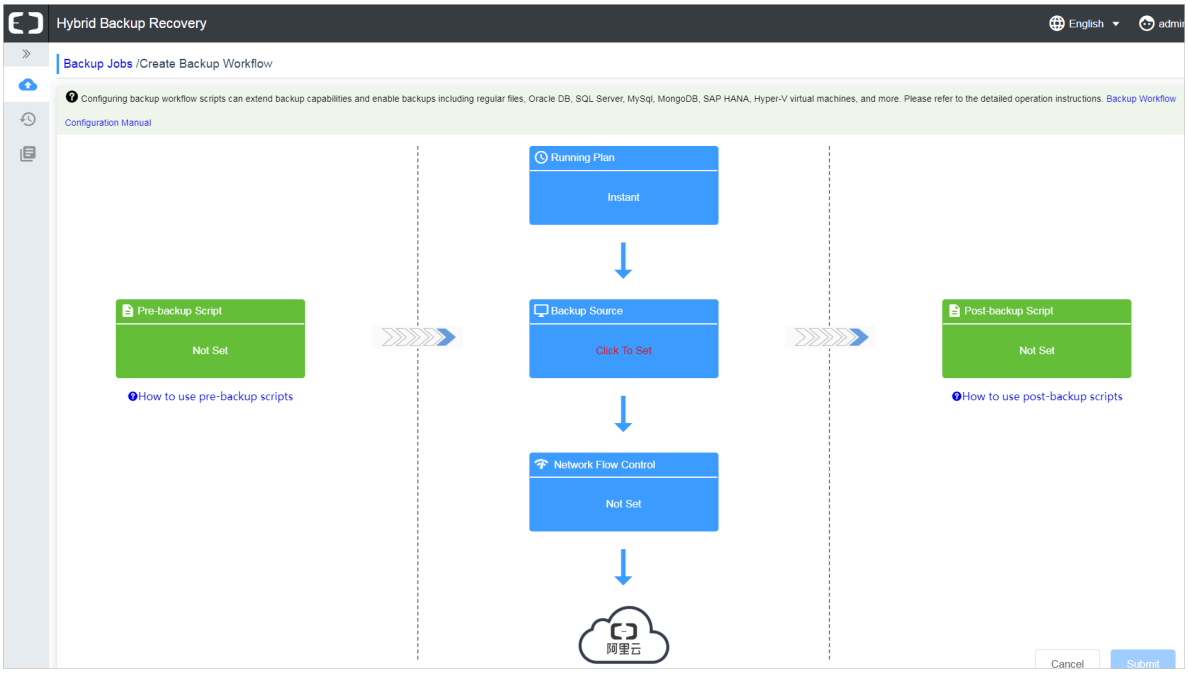
```
#!/bin/sh

#************************************************************
#* Copyright 2018 Ali Corporation, All Rights Reserved
#************************************************************

# Change following values according to the configuration of your environment.
HDB_SQL=/usr/sap/<SID>/HDB01/exe/hdbsql # path to the hana sql client program
INSTANCE_ID=0                           # instance number
HANA_HOST=localhost                     # hostname of the master node

# credential env should be set in workflow.env
# USER_NAME
# PASSWORD
```

Post-backup script

Download the post-backup script for SAP HANA and change the path in the script to the local backup path of SAP HANA. Save the script.

Step 3: Create a backup workflow

1. Log on to the HBR backup client and click Create Backup Workflow in the upper-right corner.
2. On the Backup Jobs/Create Backup Workflow page, click Pre-backup Script.



3. In the Script Path field of the Pre-backup Script dialog box, enter the file path of the pre-backup script configured in Step 2.

> Note:
> The script path must be a maximum of 250 characters in length.

4. Click Preview to check the details of the pre-backup script and click OK.
5. On the Backup Jobs/Create Backup Workflow page, click Running Plan.
6. In the Running Plan dialog box, configure the following settings and click OK.
   - If you have a regular backup plan, click Scheduled. In the Backup Policy drop-down list, select a backup policy.
   - If you have no regular backup plan, click Instant.
7. On the Backup Jobs/Create Backup Workflow page, click Backup Source.

8. In the Backup Source dialog box, configure the following settings. Then, click OK.

Parameter	Description
Source	· Enter the path of a backup source. You can enter a maximum of eight paths, which means that you can back up data from eight directories at a time. · The path is dedicated to storing workflow-based backups. The path must be directed to an empty directory. · In the configuration of SAP HANA, set the backup path to this path. · You can enter a Universal Naming Convention (UNC) path as a source path. · Separate multiple paths with carriage returns.
Use VSS for backup (Windows only)	SAP HANA does not support the Volume Shadow Copy Service (VSS).

9. (Optional) On the Backup Jobs/Create Backup Workflow page, click Network Flow Control.

> Note:
> You can use throttling to set bandwidth limits for backing up data during peak hours to ensure business continuity. If you do not need to configure throttling, you can skip this step and the next step.

10. (Optional) In the Network Flow Control dialog box, set a period in Work Hours and a maximum bandwidth in Throttling, and then click Add. Confirm the configuration and click OK.

> Note:
> You can use throttling to set bandwidth limits for backing up data during peak hours to ensure business continuity. If you do not need to configure throttling, you can skip this step.

11. On the Backup Jobs/Create Backup Workflow page, click Post-backup Script. In the Script Path field of the Post-backup Script dialog box, enter the file path of the post-backup script configured in Step 2. Click OK.

> Note:
> The script path must be a maximum of 250 characters in length.

12. On the Backup Jobs/Create Backup Workflow page, click Submit to start a backup job.

> Note:
> - If you need to cancel a backup job, locate the running backup job on the Backup Jobs page and click Cancel next to the backup job.
> - If a backup job fails, you can locate the running job on the Backup Job page and click Retry next to the backup job. You can also click the Download icon next to the number of errors to download and view the error report.

More actions

Restore backups

Search backups

3.4 Back up MySQL

This topic describes how to use Hybrid Backup Recovery (HBR) to back up data from on-premises MySQL.

Prerequisites

You have completed the preparations.

Step 1: Create a file named workflow.env

1. Go to the installation directory of the HBR backup client and create a file named `workflow.env` in the `client` subdirectory.

> Note:
> The `workflow.env` file must be stored in the same directory as the `hybridebackup` and `ids` executable files.

2. In the `workflow . env` file, enter the username and password of a backup source in the following format:

```
USERNAME = root
PASSWORD =****
```

Step 2: Configure backup scripts

Pre-backup script

1. Download the pre-backup script for MySQL.
2. Configure and save the pre-backup script. The following section describes the parameters that need to be configured in the pre-backup script for MySQL. You can configure these parameters as required.
   - Windows

Parameter	Description
BackupDir	The local backup path of the database . You need to specify this path as the backup source.

Parameter	Description
MySQLInstallDir	The installation directory of the database.

```
#************************************************************
#* Copyright 2018 Ali Corporation, All Rights Reserved
#************************************************************

# configurations
$BackupDir = "<backup path>"
$MySQLInstallDir = "<mysql server install dir>"

# credential env should be set in workflow.env
# $Env:Username
# $Env:Password

$id = (Get-Date -Format yyyyMMdd-HHmmss)
& $MySQLInstallDir/bin/mysqldump.exe -A -Y -u $Env:Username -p"$Env:Password" > $BackupDir/mysql-$id.bak
if ($LastExitCode -ne 0) {
    throw "mysqldump exited with error $LastExitCode"
```

- Linux

  `BACKUPDIR` : the local backup path of the database. You need to specify this path as the backup source.

```
#!/bin/bash

#************************************************************
#* Copyright 2018 Ali Corporation, All Rights Reserved
#************************************************************

BACKUPDIR=<backup path>

# credential env should be set in workflow.env
# USERNAME
# PASSWORD

mysqldump -u ${USERNAME} -p"${PASSWORD}" -A -Y > ${BACKUPDIR}/mysql-$(date +%FT%T).bak
```

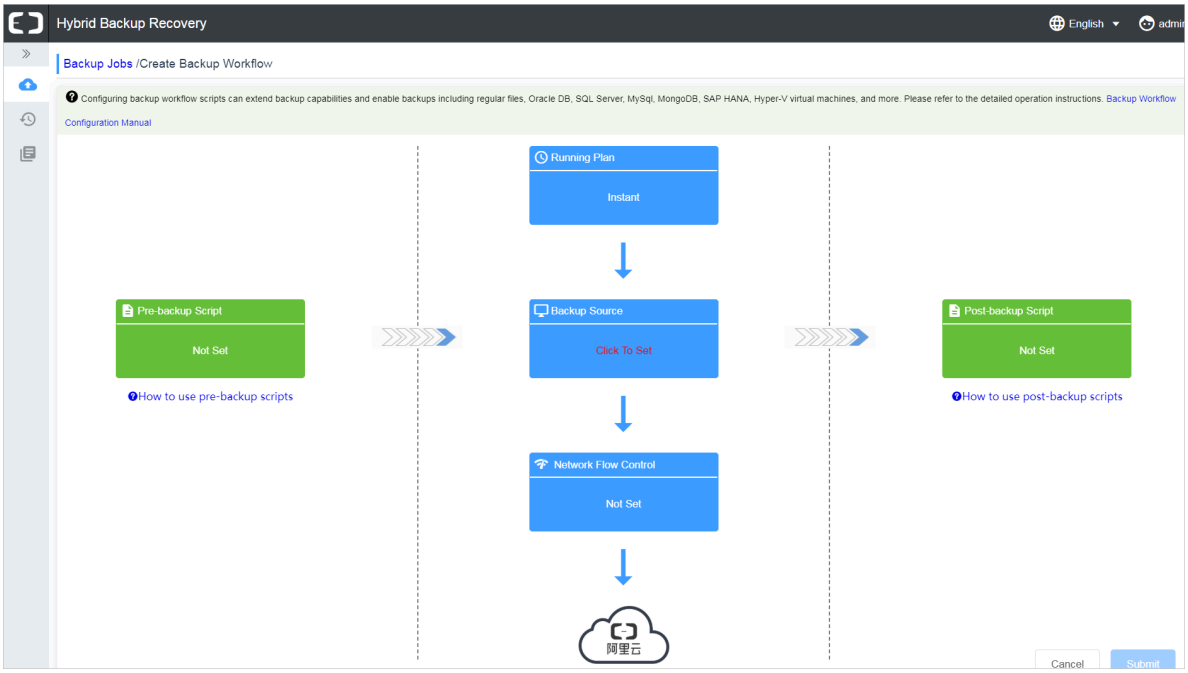
Post-backup script

Download the post-backup script for MySQL and change the path in the script to the local backup path of MySQL. Save the script.

Step 3: Create a backup workflow

1. Log on to the HBR backup client and click Create Backup Workflow in the upper-right corner.

2. On the Backup Jobs/Create Backup Workflow page, click Pre-backup Script.



3. In the Script Path field of the Pre-backup Script dialog box, enter the file path of the pre-backup script configured in Step 2.

> Note:
> The script path must be a maximum of 250 characters in length.

4. Click Preview to check the details of the pre-backup script and click OK.
5. On the Backup Jobs/Create Backup Workflow page, click Running Plan.
6. In the Running Plan dialog box, configure the following settings and click OK.
   - If you have a regular backup plan, click Scheduled. In the Backup Policy drop-down list, select a backup policy.
   - If you have no regular backup plan, click Instant.
7. On the Backup Jobs/Create Backup Workflow page, click Backup Source.

8. In the Backup Source dialog box, configure the following settings. Then, click OK.

Parameter	Description
Source	· Enter the path of a backup source. You can enter a maximum of eight paths, which means that you can back up data from eight directories at a time. · The path is dedicated to storing workflow-based backups. The path must be directed to an empty directory. · You can enter a Universal Naming Convention (UNC) path as a source path. · Separate multiple paths with carriage returns.
Use VSS for backup (Windows only)	· If data changes occur in the backup source, select this option to ensure consistency between source data and backup data. · This feature is only available for hosts running Windows. · If you select this option, you cannot back up data from multiple backup sources.

9. (Optional) On the Backup Jobs/Create Backup Workflow page, click Network Flow Control. In the Network Flow Control dialog box, set a period in Work Hours and a maximum bandwidth in Throttling, and then click Add. Confirm the configuration and click OK.

 Note:
You can use throttling to set bandwidth limits for backing up data during peak hours to ensure business continuity. If you do not need to configure throttling, you can skip this step.

10. On the Backup Jobs/Create Backup Workflow page, click Post-backup Script. In the Script Path field of the Post-backup Script dialog box, enter the directory of the post-backup script configured in Step 2. Click OK.

> Note:
> The script path must be a maximum of 250 characters in length.

11. On the Backup Jobs/Create Backup Workflow page, click Submit to start a backup job.

> Note:
> - If you need to cancel a backup job, locate the running backup job on the Backup Jobs page and click Cancel next to the backup job.
> - If a backup job fails, you can locate the running job on the Backup Job page and click Retry next to the backup job. You can also click the Download icon next to the number of errors to download and view the error report.

More actions

Restore backups

Search backups

3.5 Back up SQL Server

This topic describes how to use Hybrid Backup Recovery (HBR) to back up data from on-premises SQL Server.

Prerequisites

You have completed the preparations.

Step 1: Configure backup scripts

Pre-backup script

1. Download the pre-backup script for SQL Server.

2. Configure and save the pre-backup script. The following section describes the parameters that need to be configured in the pre-backup script for SQL Server. You can configure these parameters as required.

   · SQL Server Diff

Parameter	Description
SqlDatabase	The name of the database.
BackupDir	The local backup path of the database . You need to specify this path as the backup source.

```
#************************************************************
#* Copyright 2018 Ali Corporation, All Rights Reserved
#************************************************************

#Change following values according to the configuration of your environment.
$SqlServer = "localhost"
$SqlDatabase = "mydb"
$backupDir = "C:\backup"

Write-Host "[INFO] Start Backup-SQL-Database"
Write-Host "[INFO] Server: $SqlServer"
Write-Host "[INFO] Database: $SqlDatabase"

#Load SMO assemblies
[System.Reflection.Assembly]::LoadWithPartialName("Microsoft.SqlServer.SMO") | Out-Null
[System.Reflection.Assembly]::LoadWithPartialName("Microsoft.SqlServer.SmoExtended") | Out-Null
```

   · SQL Server Full

Parameter	Description
SqlDatabase	The name of the database.
BackupDir	The local backup path of the database . You need to specify this path as the backup source.

```
#************************************************************
#* Copyright 2018 Ali Corporation, All Rights Reserved
#************************************************************

#Change following values according to the configuration of your environment.
$SqlServer = "localhost"
$SqlDatabase = "mydb"
$backupDir = "C:\backup"

Write-Host "[INFO] Start Backup-SQL-Database"
Write-Host "[INFO] Server: $SqlServer"
Write-Host "[INFO] Database: $SqlDatabase"
```

   · SQL Server Log

Parameter	Description
SqlDatabase	The name of the database.

Parameter	Description
BackupDir	The local backup path of the database. You need to specify this path as the backup source.

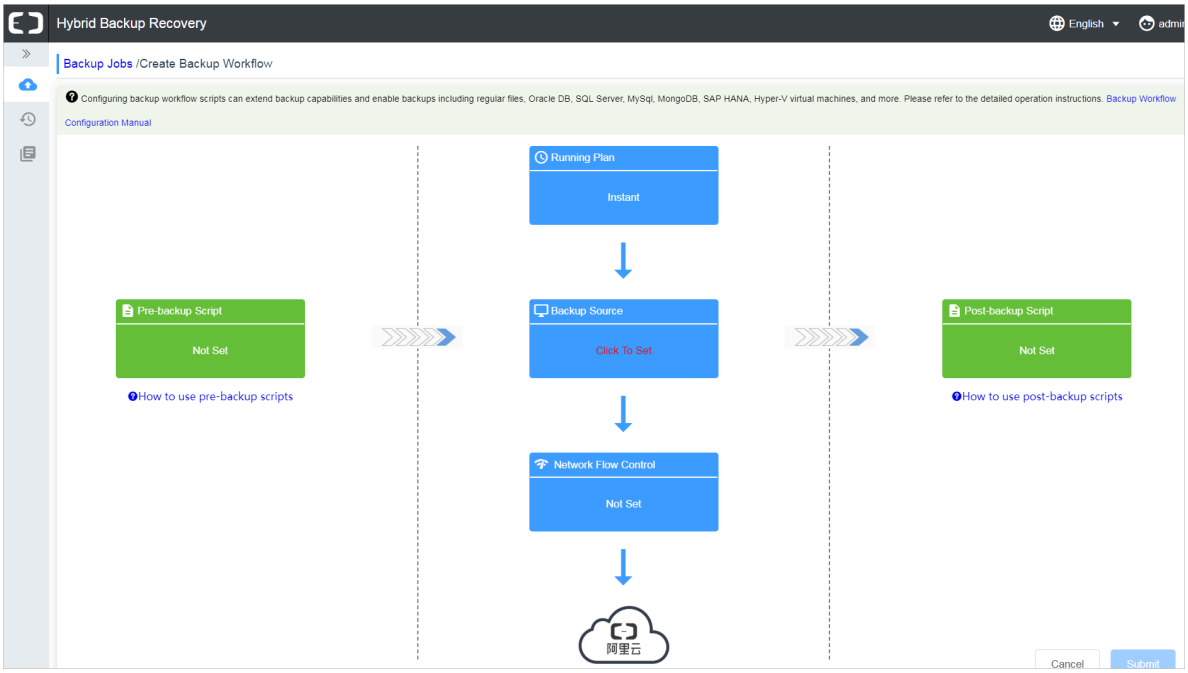
```
#*************************************************************
#* Copyright 2018 Ali Corporation, All Rights Reserved
#*************************************************************

#Change following values according to the configuration of your environment.
$SqlServer = "localhost"
$SqlDatabase = "mydb"
$backupDir = "C:\backup"

Write-Host "[INFO] Start Backup-SQL-Database"
Write-Host "[INFO] Server: $SqlServer"
Write-Host "[INFO] Database: $SqlDatabase"
```

Post-backup script

Download the post-backup script for SQL Server and change the path in the script to the local backup path of SQL Server. Save the script.

Step 2: Create a backup workflow

1. Log on to the HBR backup client and click Create Backup Workflow in the upper-right corner.
2. On the Backup Jobs/Create Backup Workflow page, click Pre-backup Script.



3. In the Script Path field of the Pre-backup Script dialog box, enter the file path of the pre-backup script configured in Step 1.

   Note:
   The script path must be a maximum of 250 characters in length.

4. Click Preview to check the details of the pre-backup script and click OK.
5. On the Backup Jobs/Create Backup Workflow page, click Running Plan.
6. In the Running Plan dialog box, configure the following settings and click OK.
   - If you have a regular backup plan, click Scheduled. In the Backup Policy drop-down list, select a backup policy.
   - If you have no regular backup plan, click Instant.
7. On the Backup Jobs/Create Backup Workflow page, click Backup Source.
8. In the Backup Source dialog box, configure the following settings. Then, click OK.

Parameter	Description
Source	· Enter the path of a backup source. You can enter a maximum of eight paths, which means that you can back up data from eight directories at a time. · The path is dedicated to storing workflow-based backups. The path must be directed to an empty directory. · You can enter a Universal Naming Convention (UNC) path as a source path. · Separate multiple paths with carriage returns.
Use VSS for backup (Windows only)	· If data changes occur in the backup source, select this option to ensure consistency between source data and backup data. · This feature is only available for hosts running Windows. · If you select this option, you cannot back up data from multiple backup sources.

9. (Optional) On the Backup Jobs/Create Backup Workflow page, click Network Flow Control. In the Network Flow Control dialog box, set a period in Work Hours and a maximum bandwidth in Throttling, and then click Add. Confirm the configuration and click OK.

    Note:
   You can use throttling to set bandwidth limits for backing up data during peak hours to ensure business continuity. If you do not need to configure throttling, you can skip this step.

10. On the Backup Jobs/Create Backup Workflow page, click Post-backup Script. In the Script Path field of the Post-backup Script dialog box, enter the file path of the post-backup script configured in Step 1. Click OK.

     Note:
    The script path must be a maximum of 250 characters in length.

11. On the Backup Jobs/Create Backup Workflow page, click Submit to start a backup job.

     Note:

    - If you need to cancel a backup job, locate the running backup job on the Backup Jobs page and click Cancel next to the backup job.
    - If a backup job fails, you can locate the running job on the Backup Job page and click Retry next to the backup job. You can also click the Download icon next to the number of errors to download and view the error report.
    - Database files of SQL Server cannot be installed on a file system that uses compression. For more database installation restrictions, see File Locations for Default and Named Instances of SQL Server.

More actions

Restore backups

Search backups

3.6 Back up data from MongoDB

This topic describes how to use Hybrid Backup Recovery (HBR) to back up data from on-premises MongoDB.

Prerequisites

You have completed the preparation.

Step 1: Create a file named workflow.env

1. Open the installation folder of an HBR backup client, create a file named `workflow.env` in the `client` subfolder.

   > Note:
   > The folder where the `workflow.env` file is located must be the same as that of the `hybridebackup` and `ids` executable files.

2. In the `workflow.env` file, enter the username and password of a backup source. This format is as follows:

```
USERNAME = root
PASSWORD =****
```

Step 2: Create a backup script

Pre-backup scripts

1. Download the pre-backup script of MongoDB.
2. Configure and save the pre-backup script. The parameters and the description of each parameter that you can configure for the pre-backup script of MongoDB are listed in the following table. You can configure these parameters as required.

   - Windows

Name	Description
BackupDir	The local directory for the database. You need to specify the directory as the backup source.
MongoDBInstallDir	The installation directory of the database.
DBHOST	127.0.0.1

Name	Description
DBPORT	The port that is used to access the database.

```
#************************************************************
#* Copyright 2018 Ali Corporation, All Rights Reserved
#************************************************************

# configurations
$BackupDir = "<backup path>"
$MongoDBInstallDir = "<mongodb install dir>"
$DBHOST = "<the host of mongo server>"
$DBPORT = "<the port of mongo server>"

# credential env should be set in workflow.env
# $Env:Username
# $Env:Password

$id = (Get-Date -Format yyyyMMdd-HHmmss)
& $MongoDBInstallDir/bin/mongodump.exe --host $DBHOST --port $DBPORT --userr
if ($LastExitCode -ne 0) {
    throw "mongodump exited with error $LastExitCode"
```

- Linux

Name	Description
BackupDir	The local directory for the database. You need to specify the directory as the backup source.
MongoDBInstallDir	The installation directory of the database.
DBHOST	127.0.0.1
DBPORT	The port that is used to access the database.

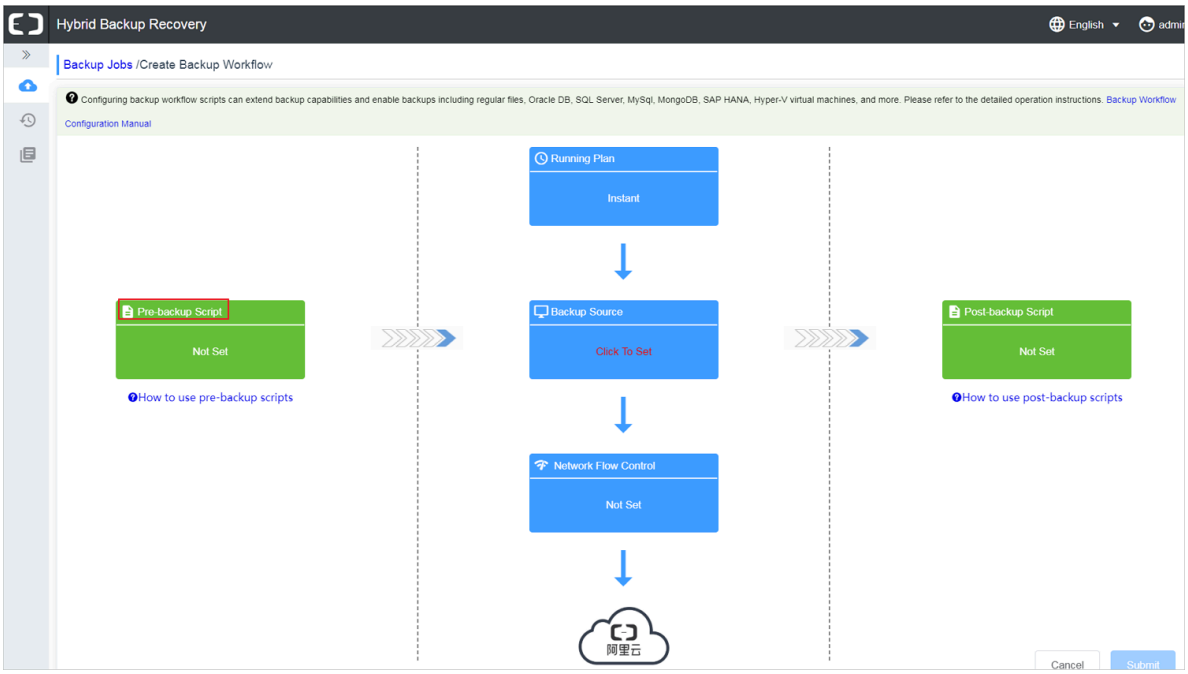
```
#!/bin/bash

#************************************************************
#* Copyright 2018 Ali Corporation, All Rights Reserved
#************************************************************

BACKUPDIR=<backup path>
DBHOST=<the host of mongo server>
DBPORT=<the port of mongo server>

# credential env should be set in workflow.env
# USERNAME
# PASSWORD

mongodump --host ${DBHOST} --port {$DBPORT} --username ${USERNAME} --password ${PASSWORD}
```

Post-backup scripts

Download the post-backup script of MongoDB and specify the local backup directory of MongoDB as the value of the BACKUPDIR parameter of the post-backup script. Save the script.

Step 3: Create a backup workflow

1. Log on to a backup client, click Create Backup Workflow in the upper-right corner.
2. On the Backup Jobs/Create Backup Workflow page, click Pre-backup Script.

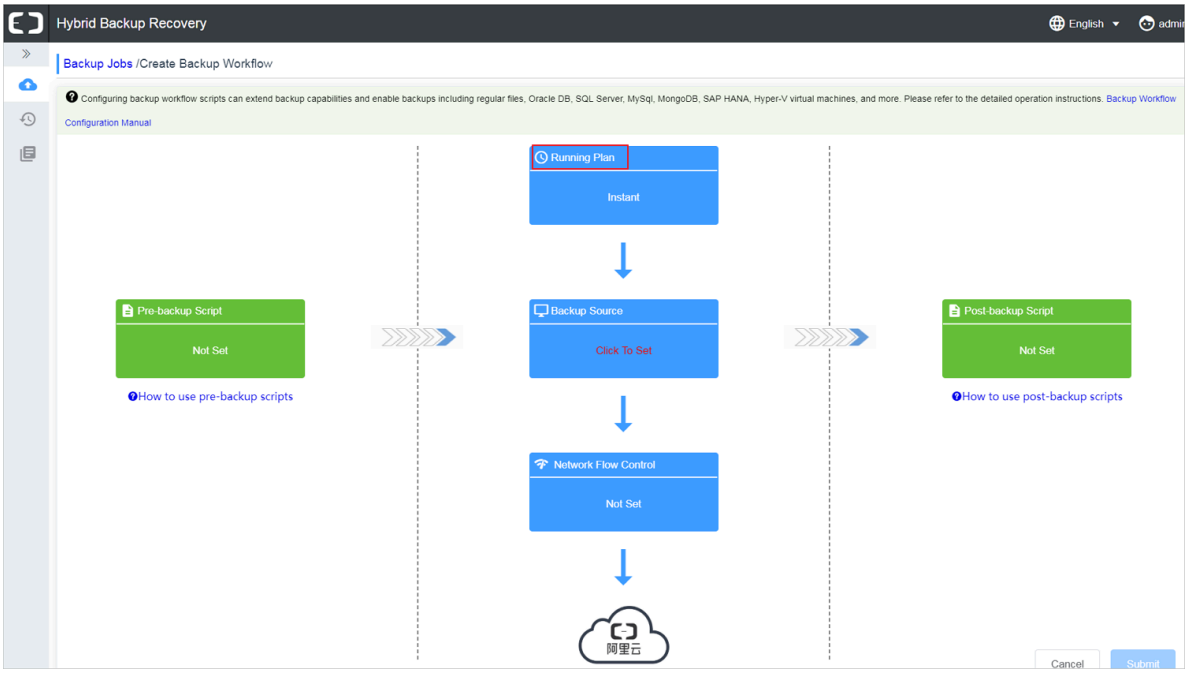


3. In the Script Path field of the Pre-backup Script dialog box, enter the directory of the pre-backup script configured in Step 2.

> **Note:**
> The script path must be a maximum of 250 characters in length.

4. Click Preview to check the details of the pre-backup script and click OK.

5. On the Backup Jobs/Create Backup Workflow page, click Running Plan.



6. In the Running Plan dialog box, configure the following settings and click OK.
   - If you have a periodical backup plan, click Scheduled。 On the Backup Policy drop-down list, select an existing backup policy.
   - If no periodical backup plan exists, click Instant.
7. On the Backup Jobs/Create Backup Workflow page, click Backup Source.
8. In the Backup Source dialog box, configure the following settings. Then, click OK.

Name	Description
Source	· Enter the path of a backup source. You can enter a maximum of eight paths, which means that you can back up data from eight paths at a time. · The path is dedicated to storing workflow-based backups. The path must be directed to an empty folder. · You can enter a universal naming convention (UNC) path. · Separate multiple paths with carriage returns.

Name	Description
Use VSS for backup (Windows only)	· If data changes occur in the backup source, select this option to ensure consistency between source data and backup data. · This function is only available for hosts running Windows. · If you select this option, you cannot back up data from multiple backup sources.

9. (Optional) On the Backup Jobs/Create Backup Workflow page, click Network Flow Control. In the Network Flow Control dialog box, select a period of Work Hours and a maximum bandwidth of Throttling, and then click Add. Confirm the configuration and click OK.

   Note:
   You can use flow control to set bandwidth limits for backing up data during peak hours to ensure business continuity. If you do not need to configure flow control, you can skip this step

10. On the Backup Jobs/Create Backup Workflow page, click Post-backup Script. In the Script Path field of the Post-backup Script dialog box, enter the directory of the post-backup script configured in Step 2. Click OK.

    Note:
    The script path must be a maximum of 250 characters in length.

11. On the Backup Jobs/Create Backup Workflow page, click Submit to start a backup job.

Note:

- If you need to cancel a backup job, locate the running backup job on the Backup Jobs page and click Cancel next to the backup job.
- If a backup job fails, you can locate the running job on the Backup Job page and click Retry next to the backup job. You can also click the Download icon next to the number of errors to download and view the error report.

More actions

Restore backups

Search backups

3.7 Restore backups

This topic describes how to restore workflow-based backups.

Restore backups by using this client

Procedure

1. Log on to a Hybrid Backup Recovery (HBR) backup client.
2. In the left-side navigation pane, select Restore to open the Restore Backup / Backups page.
3. On the `Backups` tab, locate the target backup, and click Restore next to the backup.
4. In the Restore Backup dialog box, configure the required settings as described in the following table, select backups to be restored, and click Submit to restore these backups.

Name	Description
Target Folder	The target folder to which backups are restored.
File Options	· Include Files: Only selected files and folders are restored to the target folder. · Exclude Files: All files and folders are restored to the target folder except for the selected files and folders.

Restore from other clients

Procedure

1. Log on to an HBR client.
2. In the left-side navigation pane, select Restore to open the Restore Backup / Backups page.
3. In the upper-right corner of the page, click Restore From Other Client.

4. In the Restore Backup dialog box, select a client where files to be restored are located and click Next.
5. Select the version of a backup to be restored and click Next.
6. On the Restore File tab, configure the required settings as described in the following table, select files to be restored, and click Submit to restore a backup.

Name	Description
Target Folder	The target folder to which backups are restored.
File Options	· Include Files: Only selected files and folders are restored to the target folder. · Exclude Files: All files and folders are restored to the target folder except for the selected files and folders.

3.8 Search backups

When you restore a piece of data among a large number of backups, you can use the backup search function to locate the target piece of data in seconds.

Turn on the backup search function

1. Log on to the Hybrid Backup Recovery (HBR) console.
2. In the left-side navigation pane, select Overview.
3. On the Overview page, locate the required vault where you need to turn on the backup search function.
4. In the upper-right corner of the vault, click Settings.
5. In the Vault Setting dialog box, turn on `Backup Search`.

> Note:
> The backup search function is only available for vaults that are located in the China (Hangzhou) and China (Shanghai) regions.

Search backups

1. Log on to an HBR backup client.
2. In the left-side navigation pane, select Restore.
3. On the Restore Backup / Backups page, select the Search Backups tab.

4. Enter a keyword or relative path of a file that you need to restore and click Search.

   Note:

   - You can search for a file by using the full name of the file. You must enclose the full name with a pair of quotation marks (").
   - When searching for a file by a relative path, you must use forward slashes (/) as delimiters. For example, A/test.text.

5. You can also turn on Advanced Search in the upper-right corner of the page. Configure one or more of the following settings and click Search.

Name	Description
File Type	Select File or Folder as required.
Modify Time	The last modification time of a file. The time is accurate to the second. If you need to clear the specified time, click X next to the time.
File Size	You can specify a range of backup sizes. Valid values : KB, MB, and GB. The minimum size of a backup is 0 KB.
Backup Time	A time period in which the target backup is completed. You must specify the start time and the end time of the period. The time is accurate to the second. If you need to clear the specified time, click X next to the time.

   If you need to cancel the previous settings, click Reset.

6. Search results are displayed at the bottom of the Search Backups page, locate the backup you need to restore and click Restore next to the backup.
7. In the Restore Backup dialog box, enter the target folder to which you need to restore the file, and click Submit to restore the backup.

3.9 Backup alerts

Backup alerts provide you with backup 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 custom alert methods, contacts, or contact groups.

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

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

1. Log on to the Hybrid Backup Recovery (HBR) console.
2. In the left-side navigation pane, select Alarm Contact.
3. Select the `Alarm Contact` tab.
4. In the upper-right corner, click New Contact.
5. In the New Contact dialog box, enter the `Contact Name` .
6. Select a `Contact Method` as required and perform the following actions:
   - Email

     If you select Email as a contact method, enter the Contact Email and then click Send Verification. Log on to the specified mailbox to view the verification code, go 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 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 contacts and the related information of each contact.
- You can click Edit to modify the email and mobile number.
- You cannot delete a contact that is selected to receive alerts or added to a contact group.

Create an alarm contact group

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

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

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

Create custom alarm policies

You can create the following types of alarm policies:

- Vault-level alarm policies

  A vault-level alarm policy applies to all the backup clients of a vault. The backup clients include those installed on ECS instances, local hosts, and local virtual machines. If you create an alarm policy for the vault where a client is located, the alarm policy of the vault applies to the client by default.

- Instance-level alarm policies

  An instance-level alarm policy applies to the backup client installed on a specific instance. After you create an alarm policy for a client, the client no longer uses the alarm policy of the vault or the default alarm policy.

 Note:
If you create no alarm policy for a vault or a client, email alerts are sent to an Alibaba Cloud account.

Create a vault-level alarm policy

Proceed as follows:

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

     If you select this option, no alert will be sent when an alarm occurs on a client or ECS instance that is located in the vault.
   - Default Notification

     If you select this option, alerts for the vault are sent to an Alibaba Cloud account by using emails.
   - Customized Notification

     If you select this option, you can select one or more contacts or contact groups. After you complete the configuration, alerts for the vault are set to the selected contacts or contact groups.
5. Click OK.

Create an alarm policy for a client

Proceed as follows:

1. Log on to the HBR console.
2. Locate a client for which you need to create an alarm policy, choose More > Alarm Setting next to the client.
3. In the Alarm Policy dialog box, select an `Alarm Policy` as required.

Alarm Policy	Description
Disabled	If you select this option, no alert is sent when an alarm occurs on the client.

Alarm Policy	Description
Same as Vault	The alarm policy of the vault where the client is located applies to the client.
Default Notification	Alerts for the client are sent to an Alibaba Cloud account by using emails.
Customized Notification	You can select one or more alarm contacts or alarm contact groups. After you complete the configuration, alerts for the client are sent to the selected alarm contacts or alarm contact groups.

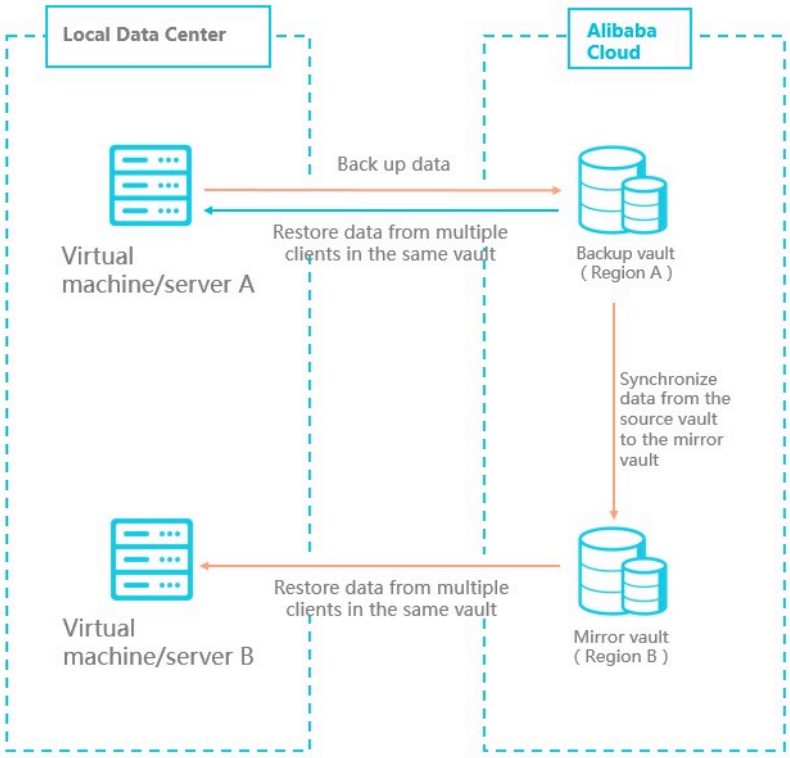
4. Click OK.

3.10 Mirror vaults

A backup vault is a Hybrid Backup Recovery (HBR) cloud warehouse used to store backup data on the cloud. Backup data from multiple clients can be stored in the same vault. You can create a remote mirror vault for a vault to meet the disaster recovery requirements.

 Note:

- After a mirror vault is created, data that is being backed up by a backup job in the source vault are synchronized to the mirror vault in real time. The historical backups of 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 from 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 always 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 backup vault for which you need to create a mirror vault, and click the icon in the upper-right corner of the backup vault.
4. In the Create Mirror Vault dialog box, select a region where the mirror vault is located.

   Note:
   For disaster recovery, you cannot select a region where the source vault is located.
5. Enter the `Vault Name`. The vault name must be less than 32 characters in length.
6. Enter the `Vault Descriptio n` as required, and then click Create.

Use a mirror vault

After a mirror vault is created, you can restore backups from the mirror vault as needed. Proceed as follows:

1. Download and install a file client on a server or virtual machine to which you need to restore data.

    Note:

   When downloading the file client, you must specify the name of the target vault as the `Vault Name`.

2. Log on to the file client on the target server or virtual machine and then restore backups from another file client.

    Note:

   You can also use the backup search function to restore data.