ALIBABA CLOUD

Alibaba Cloud

Hybrid Backup

Back up on-premises severs

Document Version: 20220304

Alibaba Cloud

Legal disclaimer

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

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

Table of Contents

1.Differences between the two versions of the on-premises file backup feature

This topic describes the differences between the two versions of the on-premises file backup feature.

Hybrid Backup Recovery (HBR) provides the latest version of the on-premises file backup feature based on the earlier versions. You can use the latest version to back up on-premises files on a more comprehensive and user-friendly interface in the HBR console. When you use the on-premises file backup feature for the first time, we recommend that you use the **latest version** of this feature.

The following table describes the differences between the two versions of the on-premises file backup feature.

Item	Earlier versions of on-premises file backup	Latest version of on-premises file backup
General backup restoration	Supported.	Supported.
Network proxy	Supported.	Supported.
Unified cloud management	Not supported.	Supported.
Visualized recovery points	Not supported.	Supported.
Preset plan templates	Not supported.	Supported.
Plan editing	Only source paths can be edited.	Supported.

2.On-premises file backup (new)

2.1. Overview

Hybrid Backup Recovery (HBR) is a fully managed online backup service that allows you to back up data to the cloud in an efficient, secure, and cost-effective manner. You can use an HBR backup client to back up files from an on-premises server or virtual machine (VM) in the HBR console. You can then restore the files if they are lost or damaged.

You can perform the following operations to back up files from and restore files to on-premises servers or VMs:

- Prepare for a data backup
- Back up files
- Restore files

For more information about how to back up files from ECS instances, see Overview.

2.2. Prepare for a data backup

You can use Hybrid Backup Recovery (HBR) clients to back up files from on-premises servers or virtual machines (VMs). You can also restore the files based on your business requirements. This topic describes how to prepare for a data backup.

Context

You can use different HBR clients based on the actual scenarios. You can use the following methods to activate HBR clients:

- HBR clients for Windows can only be manually activated.
- HBR clients for Linux can be automatically or manually activated.

Prepare an AccessKey pair for a RAM user (Recommended)

Resource Access Management (RAM) is an Alibaba Cloud service that allows you to manage user identities and control access to resources. RAM allows you to create and manage multiple identities within an Alibaba Cloud account and grant different permissions to a single identity or a group of identities. This way, you can authorize different identities to access different Alibaba Cloud resources.

An AccessKey pair is required when you activate an HBR client. The AccessKey pair is an identity credential. If the AccessKey pair of your Alibaba Cloud account is leaked, all cloud resources that belong to the account are exposed to risks. Therefore, we recommend that you use the AccessKey pair of a RAM user to activate HBR clients. For information about how to create a RAM user and how to create an AccessKey pair for the RAM user, see Create a RAM user and Create an AccessKey pair for a RAM user.

Download and activate an HBR client for Windows

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > On-Premises Backup**.
3. In the top navigation bar, select a region.
4. Select file backup as the backup type.
   - If you are not using the latest version of backup client, click **File (New)** on the **On-Premises**

- If you are not using the latest version of backup client, click **File (New)** on the **On-Premises Backup** page.
- If you are using the latest version of backup client, click **File** on the **On-Premises Backup** page.

5. In the upper-right corner of the page, click **Add Client**.
6. Download the HBR client for Windows.

   You can download the installation package of the HBR client for **Windows (64-bit)** or **Windows (32-bit)**. Record the activation code. The activation code is used to install and activate the client.
7. Install and activate the HBR client for Windows.
   i. Double-click the installation package of the HBR client and select a language for installation.
   ii. Select the path in which you want to install the client and click **Next**.
   iii. Select **Local client connecting to Alibaba Cloud**, and then click **Next**.
   iv. If you want to use a proxy server, enter the IP address of the proxy server. Click **Next**.
   v. In the **Activation token** field, enter the activation code that you recorded in Step 4. Then, click **Next**.
   vi. Click **Install**.

   After the client is installed, **Activated** is displayed in the **Client Status** column on the **Clients** tab.

Download and activate an HBR client for Linux

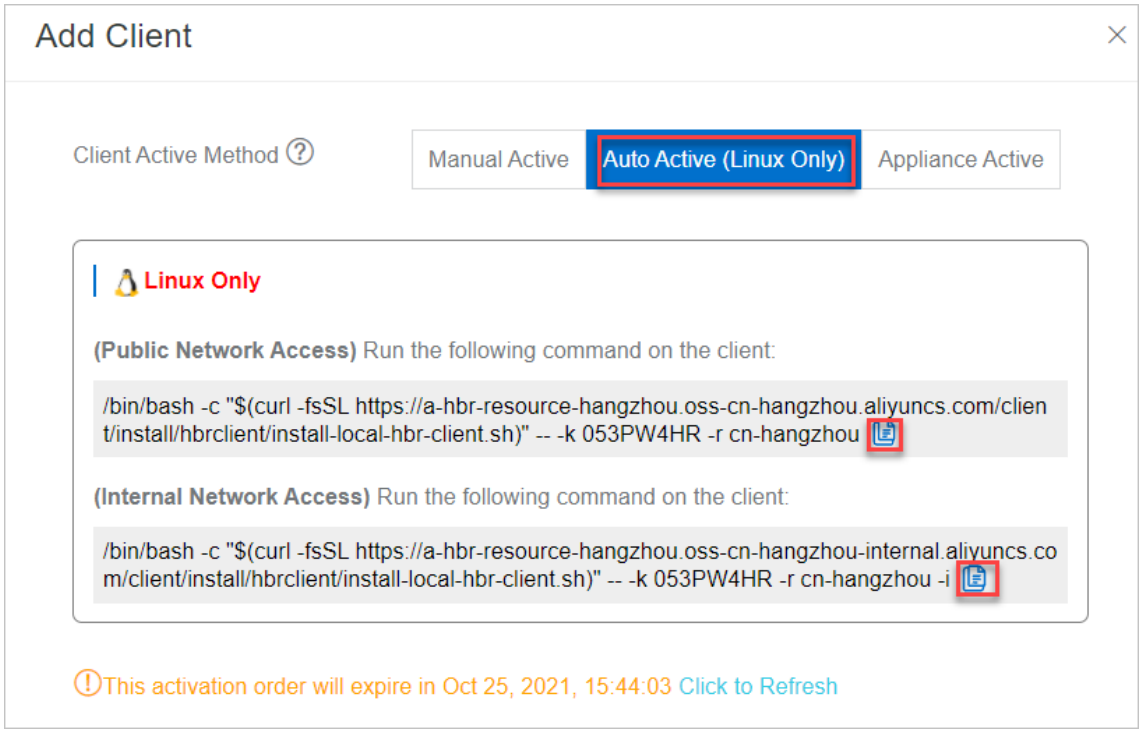
1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > On-Premises Backup**.
3. In the top navigation bar, select a region.
4. Select file backup as the backup type.
   - If you are not using the latest version of backup client, click **File (New)** on the **On-Premises Backup** page.
   - If you are using the latest version of backup client, click **File** on the **On-Premises Backup** page.
5. In the upper-right corner of the page, click **Add Client**.
6. Download and decompress the HBR client for Linux.

   You can download the installation package of the HBR client for **Linux (64-bit)** or **Linux (32-bit)**. Record the activation code. The activation code is used to install and activate the client.
7. Manually or automatically activate the HBR client for Linux.

   In the following example, `05MUE877` indicates the dynamic activation code that is obtained from the HBR console.
   - Manually activate the HBR client for Linux.

     In the path to which the HBR client is decompressed, run the following command to activate the client: `./setup -t local -k 05MUE877`.
   - Automatically activate the HBR client for Linux.

     In the Add Client panel, click **Auto Active (Linux Only)** and copy one of the commands based on your network. Then, paste and run the command that you copied on the client for Linux to activate the client.



2.3. Back up files

This topic describes how to use Hybrid Backup Recovery (HBR) to back up files from an on-premises server.

Prerequisites

The preparations for data backup are completed. For more information, see Prepare for a data backup.

Create a backup plan

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > On-Premises Backup**.
3. In the top navigation bar, select a region.
4. Select file backup as the backup type.
   - If you are not using the latest version of backup client, click **File (New)** on the **On-Premises Backup** page.
   - If you are using the latest version of backup client, click **File** on the **On-Premises Backup** page.
5. Click **Back Up** in the Actions column corresponding to the backup client that you want to use.
6. In the **Create Backup Plan** panel, set the parameters and click **OK**.

Parameter	Description

Parameter	Description
Backup Vault	If you have created backup vaults, click **Select Vault** and select a backup vault from the Vault Name drop-down list. If you have not created backup vaults, click **Create Vault** and specify Vault Name. The vault name must be 1 to 64 characters in length. **Note** A backup vault is a repository in which HBR stores backup data in the cloud. You can back up files from multiple backup clients to a backup vault. Backup vaults can reside in different regions. You can select or create a backup vault only in the specified region.
Vault Name	The name of the backup vault that stores the files.
Basic Settings	
Plan Name	The name of the backup plan. By default, a random name is used.
Backup Rules	Select **All Folders** or **Specified Folders**. ○ If you select **All Folders**, you must turn on or off **Exclude System Folders**. ■ If you turn on **Exclude System Folders**, the system folders of Windows and Linux ECS instances are not backed up. You can move the pointer over the icon to the right of **Exclude System Folders** to view the system folders in Windows and Linux. ■ If you turn off **Exclude System Folders**, all folders of the ECS instances are backed up. ○ If you select **Specified Folders**, you must enter the names of system folders in the **Source Paths** field. Specify backup paths based on the following rules: ■ If you do not use wildcards (*), you can enter up to eight backup paths. ■ If you use wildcards (*), you can enter only a single path. The path can be in the `/*/*` format. ■ Only absolute paths are supported, such as paths that start with `/`, `\\`, `C:\`, or `D:\`. ■ If you use Volume Shadow Copy Service (VSS), you can enter only one path. UNC paths and wildcards (*) are not supported. You cannot exclude files from the backup plan. ■ If you use Universal Naming Conversion (UNC), VSS paths and wildcards (*) are not supported. You cannot exclude files from the backup plan. If a UNC path is specified, HBR does not back up the access control list (ACL) of Windows.

Parameter	Description
Exclude System Folders	If you turn on **Exclude System Folders**, system folders are not backed up.
Backup File Type	Select **All Types** or **Specified Type**. If you select **Specified Type**, you must select the types of the files you want to back up from the **Select File Type** drop-down list.
Advanced Rule Mode	
Source Paths	This parameter is required only if you turn on **Advanced Rule Mode**. You can specify custom backup paths. Specify backup paths based on the following rules: ○ If you do not use wildcards (*), you can enter up to eight backup paths. ○ If you use wildcards (*), you can enter only a single path. The path can be in the `/*/*` format. ○ Only absolute paths are supported, such as paths that start with `/`, `\\`, `C:\`, or `D:\`. ○ If you use Volume Shadow Copy Service (VSS), you can enter only one path. UNC paths and wildcards (*) are not supported. You cannot exclude files from the backup plan. ○ If you use Universal Naming Conversion (UNC), VSS paths and wildcards (*) are not supported. You cannot exclude files from the backup plan. If a UNC path is specified, HBR does not back up the access control list (ACL) of Windows. ○
Backup Rule	This parameter is required only if you turn on **Advanced Rule Mode**. ○ **Include All Files**: All files are backed up. ○ **Include Files** or **Exclude Files**: In the text box, enter the paths to the folders and files that you want to back up.
Time Settings	
Start Time	The time at which the backup plan starts. The time is accurate to seconds.
Backup Interval	The interval at which incremental backup is performed. Unit: hours, days, or weeks.
Retention Policy	Select **Limited** or **Permanent**. If you select **Limited**, you must select the types of the files that you want to back up from the **Select File Type** drop-down list. If you select **Permanent**, backup files are permanently retained.

Parameter	Description
Retention Period	The retention period of backup data. Unit: days, weeks, months, or years.
Use VSS	Specify whether to use Windows VSS to define a backup path. **Note** If you use VSS, you cannot back up files from multiple paths or UNC paths. You cannot use wildcards (*) or exclude files.
Enable Traffic Shaping	Specify whether to enable traffic shaping. You can limit the bandwidth used for data backup during peak hours to guarantee business continuity. If you enable traffic shaping, you must select the Time Range (Hour) based on your requirements, enter the Max Bandwidth (MB) for backup during the specified time range, and then click **Add**.

What to do next

- Use HTTPS to transmit data

  If you use HTTPS to transmit data, the performance of data transmission is compromised. If you modify the setting of this parameter, the modification takes effect on the next backup or restore job.

  After data is encrypted and stored in the backup vault, you can choose **More > Client Settings** in the Actions columns and select whether to use HTTPS to transmit data.

- Configure a backup alert policy

  You can choose **More > Alert Settings** in the Action columns and then select a backup alert policy. The following table describes the alert policies.

Alert policy	Description
Disabled	The backup client does not send alert notifications.
Same as Vault	The backup client sends alert notifications in the same way as the backup vault.
Default	The backup client sends alert notifications to the owner of the Alibaba Cloud account by using emails.
Custom	If you select this option, you must select one or more contacts or contact groups. Then, the backup client sends alert notifications to the selected contacts and contact groups.

- Delete a backup

If you delete a backup, all backup data generated by the backup client is deleted and all backup and restore jobs that are being performed by the client fail. Before you delete a backup client, make sure that the backup data generated by the backup client is no longer required. In addition, make sure that no backup or restore jobs are being performed by the backup client.

You can choose **More > Delete Backup** in the Actions column and then click OK to delete the backup data that is no longer required.

What's next

Restore files

2.4. Restore files

You can restore files that are backed up on an HBR backup client to an on-premises server. You can also restore files that are backed up on another backup client in the same backup vault to the current backup client.

Prerequisites

The files on the on-premises server are backed up. For more information, see Back up files.

Create a restore job

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > On-Premises Backup**.
3. In the top navigation bar, select a region.
4. Select file backup as the backup type.
   - If you are not using the latest version of backup client, click **File (New)** on the **On-Premises Backup** page.
   - If you are using the latest version of backup client, click **File** on the **On-Premises Backup** page.
5. On the **Backup Plans** tab, click the + icon on the left of a completed backup plan.
6. Click a point in time to which a backup can be restored, and click **Restore**.
7. In the **Create Restore Job** dialog box, configure the following settings as prompted:

i. Set the restoration parameters and click **Next**.

Parameter	Description

Restore Items	The files or directories that you want to restore.
	■ **Include All Files**: All files on the client are restored.
	■ **Include Files**: Select the files or folders that you want to restore.
	You can also click **Enter Paths** to specify the files that you want to restore. In the text box, enter the paths to the folders or files that you want to restore. HBR restores files in the client based on the specified restore policy.
	In the text box, enter one path in each line and ensure that each path starts with the lowest-level folder in the directory that is backed up. For example, if the files in *folder/test/data* are backed up and you want to restore the file.txt and abc.png files in the data folder, enter the following paths:
	`/data/file.txt`
	`/data/abc.png`
	■ **Exclude Files**: Select the files or folders that you do not want to restore.
	You can also click **Enter Paths** to specify the files that you do not want to restore. In the text box, enter the paths to the folders or files that you do not want to restore. You must enter the paths in the same format as you enter those of folders or files that you want to restore.

ii. Configure a destination for data restoration and click **Next**.

Parameter	Description
Destination Type	Select the type of the destination to which files are restored. ■ ECS Client: restores files to an ECS instance. ■ On-premises Client: restores files to an on-premises server.
Client Name	The client to which files are restored.

iii. Specify the recovery path and click **Start Restore**.

Parameter	Description
Restore Path Type	■ **Specify Path**: restores files to a path that you specify. ■ **Origin Path**: restores files to the path from which the files are backed up.
Destination Path	This parameter is required only if the **Restore Path Type** parameter is set to **Specify Path**. You can specify a path to which files are restored.

After the restore job is created, you can view the job progress in the **Status** column on the **Restore Jobs** tab.

2.5. Configure alert notifications

This topic describes how to configure alert notifications. If a backup attempt fails or a backup client is disconnected from the server, Hybrid Backup Recovery (HBR) sends alert notifications to the owner of the Alibaba Cloud account by default. You can customize notification contacts, contact groups, and methods.

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

Create a notification contact

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

1. Log on to the HBR console.
2. In the left-side navigation pane, click **Notification Contacts**.
3. On the Notification Contacts page, click the **Contacts** tab.
4. In the upper-right corner, click **Create Contact**.
5. In the **Create Contact** panel, specify the Contact Name parameter.
6. Select **Email** as Notification Methods.

   After you select Email, enter an email address in the **Email** field and click **Send**. Log on to the specified email box and copy the verification code. Then, paste the code in the Verification Code field in the HBR console.
7. Click **OK**.

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

Create a contact group

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

1. Log on to the HBR console.
2. In the left-side navigation pane, click **Notification Contacts**.
3. On the Notification Contacts page, click the **Groups** tab.
4. In the upper-right corner, click **Create Group**.
5. In the **Create Group** pane, specify a group name.
6. Select the contacts that you want to add to the group and click the > button. Then, the selected contacts are added to the Selected Contacts section.
7. Click **OK**.

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

Create an alert policy

You can create the following types of alert policies:

> **Note** By default, HBR sends alert notifications to the owner of the Alibaba Cloud account by using E-mails.

- Configure an alert policy for a vault

  You can configure an alert policy for a vault. The alert policy applies to all the backup clients that are associated with the vault. The backup clients include those used to back up ECS instances, on-premises files, and on-premises virtual machines (VMs). If you do not configure alert policies for the backup clients, the backup clients use the alert policy of the vault by default. To configure an alert policy for a vault, perform the following steps:

  i. Log on to the HBR console.
  ii. On the **Overview** page, find the vault.
  iii. In the upper-right corner of the vault, choose **Settings > Modify Backup Vault** .
  iv. In the **Modify Backup Vault** panel, select an alert policy as needed.

Alert policy	Description

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

v. Click **OK**.

- Configure an alert policy for a backup client

  You can configure an alert policy for a backup client. After you create an alert policy for a backup client, the backup client no longer uses the default alert policy, or the alert policy of the associated vault. To configure an alert policy for a backup client, perform the following steps:

  i. Log on to the HBR console.
  ii. In the left-side navigation pane, choose **Backup > On-Premises Backup**.
  iii. On the **File** page, find the client, and choose **More > Alert Settings** in the Actions column.
  iv. In the **Alert Settings** panel, select an alert policy as needed.

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

  v. Click **OK**.

2.6. Restore files across regions by using an image repository

This topic describes how to restore files across regions by using an image repository. An image repository is a repository where Hybrid Backup Recovery (HBR) stores backup data in the cloud. You can create a remote image repository for a backup vault to meet disaster recovery requirements. When necessary, you can use the remote image repository to restore data across regions.

> **Note**
>
> - After a mirror vault is created, backup data in the backup vault is synchronized to the mirror vault in real time. The historical backup data in the backup vault starts to be synchronized to the mirror vault 90 minutes after the mirror vault is created.
> - You can create only one mirror vault for each backup vault.
> - You can restore the backup data that is stored in a mirror vault but cannot back up the data in a mirror vault.
> - You must delete a mirror vault before you can delete the corresponding backup vault.
> - You can create a backup vault when you create a backup client.

Create a mirror vault

To create a mirror vault, perform the following steps:

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

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

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

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

Restore files from a backup stored in a mirror vault

Before you restore files that is stored in a mirror vault, perform the following steps to install a backup client for files on the destination server or virtual machine (VM) and add the client to the mirror vault.

1. Download and install a file backup client on the destination server or VM.

   > **Note** Before you download a backup client, you must create a client. When you create the client, select the mirror vault.

2. Log on to the backup client on the destination server or VM, and restore files from another client.

   > **Note** To find the files that you want to restore, you can use the backup search feature.

2.7. Use tags

You can use tags to identify resources. Tags allow enterprises and individuals to categorize Elastic Computing Service (ECS) resources and simplify the search and management of resources. This topic describes how to use the tagging feature to back up files from on-premises clients.

Prerequisites

Authorization is completed in Resource Access Management (RAM) and a file backup client is installed. For more information, see Prepare for a data backup.

Context

You can create different tags for different on-premises clients. For example, if you manage teams or projects, you can create tags based on department or project and use these tags to categorize your instances. For example, you can create a tag named `project:a` for a project. This way, you can filter on-premises clients based on the tag when you maintain your on-premises clients.

Usage notes

- Each tag consists of a key-value pair.
- A tag must be unique.

  For example, the `company:a` tag is added to a backup vault. If you add the `company:b` tag to the backup vault, the company:a tag is replaced with the `company:b` tag.
- Tags are not shared across regions. For example, tags that are created in the China (Hangzhou) region are invisible to the China (Shanghai) region.

Limits

When you create tags, take note of the following limits:

Item	Limit
The maximum length of a key	128 characters
The maximum length of a value	128 characters
The maximum number of custom tags that you can add to a resource	20
The key of a tag	• The key cannot start with `aliyun` or `acs:`. • The key cannot contain `http://` or `https://`. • The key cannot be an empty string.
The value of a tag	A tag value cannot contain `http://` or `https://`.

Create tags

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > On-Premises Backup**.
3. In the top navigation bar, select a region.
4. On the **On-Premises Backup** page, click **File**.

5. In the **Tags** column, click the icon next to the name or ID of the client for which you want to create tags.
6. In the dialog box that appears, click **Edit**.
7. In the **Key** and **Value** fields, enter the key-value pair of a tag and click **Save**.

   If you want to create more than one tags, click **Add a row** to specify the key-value pair of a new tag.

Search for a resource by a tag

On the right of the **Clients** tab, select **Client Tags** from the drop-down list and enter the tag information in the search box. Then, click the **Search** icon.

- You can search for a resource by using a key, as shown in the following example:

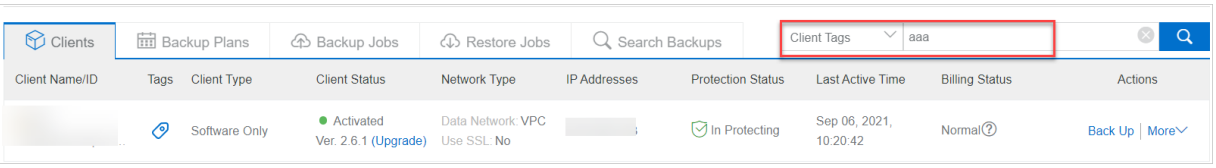
```
aaa
```

- You can search for a resource by using a key-value pair, as shown in the following example:

```
aaa:bbb
```

- You can search for a resource by using multiple key-value pairs, as shown in the following example:

```
aaa:bbb,ccc:ddd
```



3.Earlier versions of on-premises file backup

3.1. Overview

Hybrid Backup Recovery (HBR) is a fully managed online backup service that allows you to back up data to the cloud in an efficient, secure, and cost-effective way. You can use an HBR backup client to back up files from an on-premises server or virtual machine (VM). You can then restore the files when they are lost or damaged.

You can use the following procedure to back up files from an on-premises server:

- Prepare for backup.
- Back up files.
- Restore files.

For information about other features of on-premises file backup, see the following topics:

- Search backups
- Configure alert notifications
- Restore data across regions by using a mirror vault

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

3.2. Preparations

You can use Hybrid Backup Recovery (HBR) to back up files from on-premises servers or VMs. You can then restore the files if needed. This topic describes the preparations that you must make before backup.

Background information

Before you use HBR to back up files from on-premises servers or VMs, note the following information:

- You can also back up files from Elastic Compute Service (ECS) instances. For more information, see Back up files in ECS.
- To achieve the optimal backup performance, we recommend that you run a backup client on a host that has the following configurations: 64-bit processors, two or more CPU cores, and more than 8 GB available memory.
- The volume of data that can be backed up depends on the available memory. If a host has 4 GB available memory, a maximum of one million files or 8 TB data can be backed up.

(Recommended) Prepare an AccessKey pair for a RAM user

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

An AccessKey pair is required when you activate a backup client. The AccessKey pair is an identity credential. If an AccessKey pair of your Alibaba Cloud account is used, all cloud resources that belong to the account are exposed to risks. Therefore, we recommend that you use an AccessKey pair of a RAM user to activate backup clients. Before you back up data, make sure that a RAM user is created and an AccessKey pair is created for the RAM user. For more information, see Create a RAM user and Create an AccessKey pair for a RAM user.

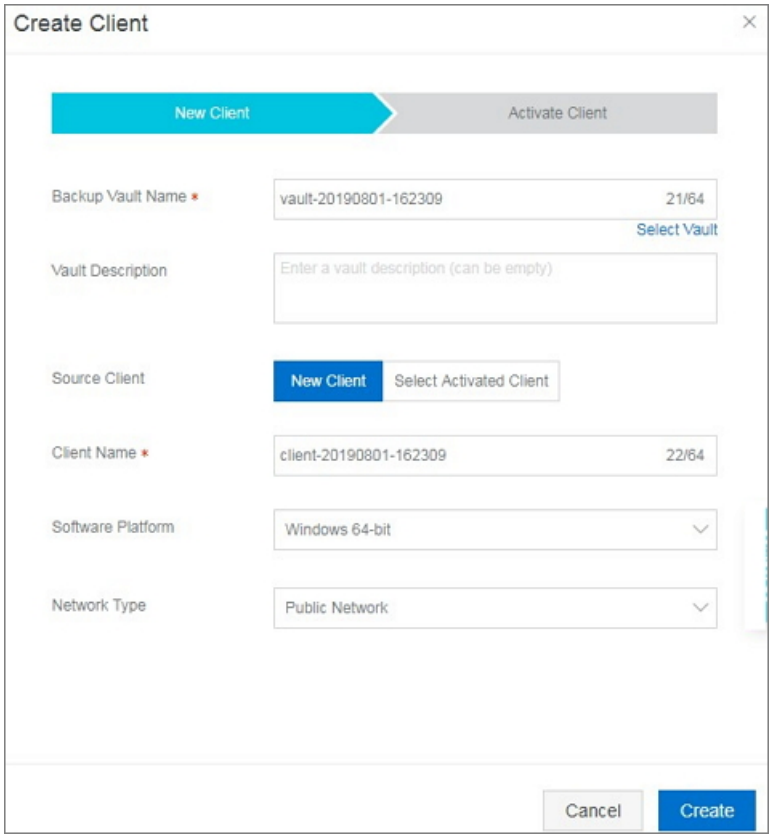
Step 1: Create a backup client

Before you back up and restore files for an on-premises server or VM, you must install a backup client on the on-premises server or VM. To create a backup client in the HBR console and download the installation package of the client, perform the following steps:

1. Log on to the HBR console.

   If your server or VM runs a Linux operating system that does not provide a graphical user interface (GUI), use an intermediate host that provides a GUI as an agent to log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > On-Premises Server Backup > File**.
3. In the top navigation bar, select the region where you want to store backup data.

   > **Note**
   > - If you use a virtual private cloud (VPC), select the region of the VPC. This guarantees a high backup speed.
   > - If you do not use a VPC and you need to achieve optimal backup performance, select a region that is close to the location of the data that you want to back up.
   > - If you do not use a VPC and you need to implement disaster recovery, select a region that is distant from the location of the data that you want to back up.
4. In the upper-right corner of the On-Premises Backup page, click **Add Client**.
5. In the **Add Client** pane, set the parameters.



The following table describes the parameters.

Parameter	Description
Backup Vault	The backup vault where you want to store the backup data. A backup vault is a repository that HBR uses to store backup data. You can use a single vault to store backup data that is received from multiple backup clients. Backup vaults reside in different regions. You can select or create only a backup vault in the current region. ○ If you have created backup vaults, click **Select Vault**, and select a backup vault from the **Vault Name** drop-down list. ○ If you have not created backup vaults, click **Create Vault** and specify the **Vault Name** field. The name must be 1 to 64 characters in length.
Backup Client	The backup client that you want to add. You can select an activated client or create a client.
Client Name	The name of the backup client. The name must be 1 to 64 characters in length.
Software Platform	The operating system that is running on the server or VM from which you want to back up data. Valid values: ○ Windows 32-bit ○ Windows 64-bit ○ Linux 32-bit ○ Linux 64-bit

Parameter	Description
Network Type	○ **Virtual Private Cloud (VPC)**: Select this option if the server or VM from which you want to back up data resides in a VPC and the VPC is in the same region as the backup vault. ○ **Internet**: Select this option if no VPCs are available.
Use HTTPS	Specifies whether to use HTTPS for encrypted data transmission. Note that HTTPS compromises the performance of data transmission. Data that is stored in the backup vault is encrypted, regardless of the setting of this switch. If you modify the setting of this parameter, the modification takes effect on the next restore job.

6. Click **Create**. Then, click **Download Client**.

> **Note** The backup client is used to connect your server or VM to HBR. You can also download the client from the client list.

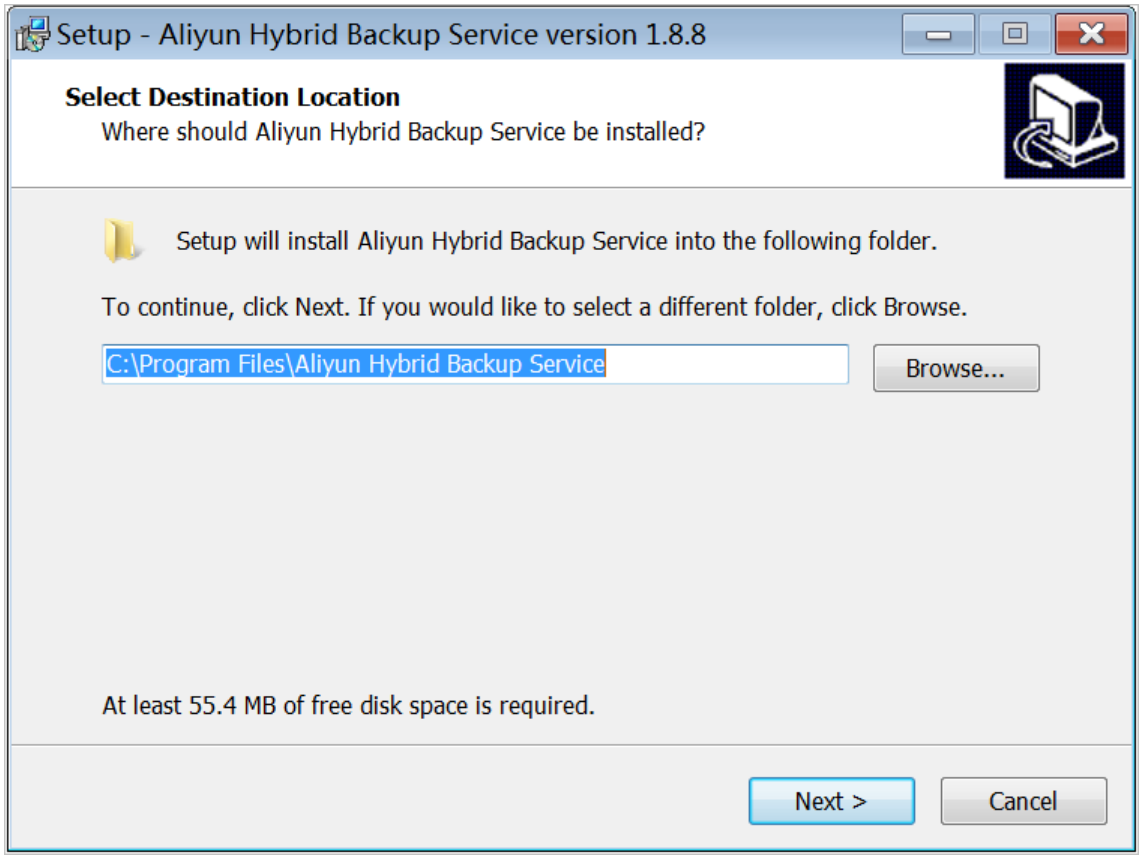
Step 2: Install and activate the backup client

After you download the installation package of a file backup client, perform the following steps to install and activate the client:

1. Select an installation directory, decompress the installation package, and then install the backup client.

> **Note** Make sure that enough space is available in the installation directory because both operational logs and an executable file are saved in the installation directory.

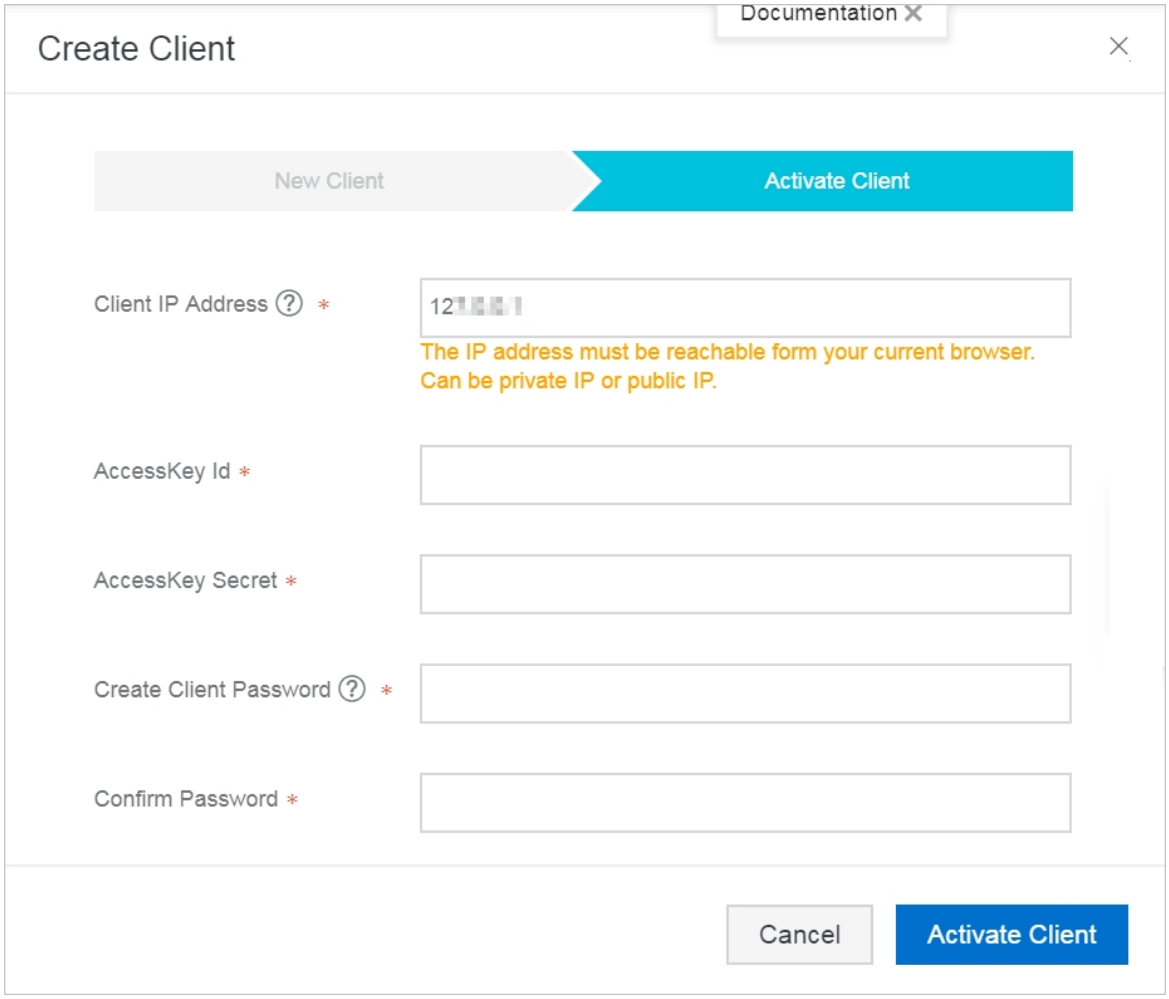
   - If your server or VM runs Windows, run the executable file that is decompressed from the installation package, select an installation directory, and then follow the instructions to install the client.



- If your server or VM runs Linux, decompress the installation package to a specified directory 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. Activate the backup client. Log on to the HBR console. On the On-Premises Backup page, click **File**. Find the backup client, and choose **More > Activate Client** in the Actions column. In the Activate Client step, set the parameters. The following table describes the parameters.



Note Make sure that the backup client is installed before you activate the client.

Parameter	Required	Description
Client IP Address	Yes	The IP address of the backup client that your current host can access. You can specify an internal IP address or an Internet IP address. For example, the IP address can be 127.0.0.1 (default), 12.34.56.78:8011, or 87.65.43.21:8443. **Note** The IP address must be reachable from your browser in use.
AccessKey Id	Yes	The AccessKey ID and AccessKey secret of the RAM user that is used to access HBR. For more information, see How can I create an AccessKey pair for a RAM user?.
AccessKey Secret	Yes	
Client Password	Yes	The password that is used to log on to the backup client. The password must be at least six characters in length.

Parameter	Required	Description
Data Network Proxy	No	The information of the proxy server that is used to transmit backup data. **Note** You can configure a data network proxy only for a backup client whose version is 1.11.11 or later.
Control Network Type	No	The type of the network that is used to call the HBR API.
Control Network Proxy	No	The information of the proxy server that is used to call the HBR API.
Message Network Type	No	The type of the network that is used to send messages from HBR to the backup client.

3. Click **Activate Client**. The page of the backup client for files appears. You can then use the backup client to back up data.

> **Note** If the activation of a backup client fails, you can reactivate the client. For more information, see How can I reactivate a file backup client?

(Optional) Create a backup policy

Before you back up data, we recommend that you plan the backup time and backup interval based on your business requirements.

- If you do not need scheduled backup, skip this step.
- If you need scheduled backup, create a backup policy and specify the first backup time and backup interval.

To create a backup policy for a file backup client, perform the following steps:

1. Log on to the HBR backup client for files.

   Open a browser, and enter `http://localhost:8011` in the address bar. Enter the password to log on to the backup client.

   > **Note**
   > - If you are using an intermediate host, replace `localhost` with the IP address of the server or VM from which you want to back up data.
   > - Port 8011 is the default port that you can use to log on to a backup client for files. If port 8011 on the server or VM is occupied by another application, specify another port number for the file backup client. For more information, see How can I change the logon port number for a file backup client?

2. In the left-side navigation pane, click **Backup Policies**.
3. In the upper-right corner of the **Backup Polices** page, click **Create Policy**.

4. In the **Create Policy** dialog box, set Name and other parameters, and click **Submit**. The following table describes the parameters.

Parameter	Description
Name	The name of the backup policy.
Frequency	The interval at which data is backed up. Units: hours, days, or weeks.
Backup Time	The time to start the first backup. The first backup is a full backup.
Retention	The retention period of the backup data. Unit: days, months, or years. Maximum value: 3650 days (10 years).

What to do next

Back up files

3.3. Back up files

You can use Hybrid Backup Recovery (HBR) to back up files from on-premises servers or virtual machines (VMs) and restore the files if needed. HBR provides the two types of backup plans: instant and scheduled. This topic describes how to back up files from on-premises servers or VMs.

> **Note** An HBR backup client backs up files in a folder incrementally based on the specified backup policy. This means that the client only backs up files that have been added or modified since last backup. For example, after HBR backs up three files in a folder: File 1, File 2, and File 3. After the backup, File 2 is edited. Then, HBR backs up only File 2 during next backup.

Create an instant backup plan

If you need only one-time full backup, perform the following steps to create an instant backup plan:

1. Log on to an HBR backup client.
2. In the left-side navigation pane, click Backup. In the upper-right corner of the Backup Jobs page, click **Create Backup Job**.
3. On the **Basic Settings** tab of the **Create Backup Job** dialog box, set the parameters. The following table describes the parameters.

Parameter	Description

Parameter	Description
Source	The paths to the source files. Specify the paths based on the following rules: ◦ If no wildcard (*) is included, you can enter a maximum of eight source paths. ◦ If wildcards (*) are included, you can enter only one source path. The format of the path can be /*/*. ◦ Only absolute paths are supported. The paths must be start with /, \\, C:\, or D:\. **Note** ◦ You can specify only one root path. For example, you cannot specify both C:\ and D:\. ◦ If VSS backup is used, you can enter only one path. Uniform Naming Convention (UNC) paths and wildcards (*) are not supported. You cannot specify files to excluded from the backup plan. ◦ If UNC paths are used, VSS backup and wildcards (*) are not supported. You cannot specify files to excluded from the backup plan. If a UNC path is specified, HBR does not back up the access control list (ACL) of Windows.
Use VSS for backup (Windows only)	◦ Specifies whether to use Volume Shadow Copy Service (VSS) for backup. If data in the backup source changes, select this check box. VSS ensures data consistency between the source and the backup. ◦ This parameter is valid only for Windows clients. ◦ If VSS is used, you cannot back up data from multiple directories. **Note** This feature is unavailable if the backup source resides on a volume of the exFAT format.
	The rule that specifies the files to be excluded from the backup plan. Select **All Files** or **Exclude Files**.

Parameter	Description
Backup Rule	If you select **Exclude Files**, specify the paths to files that you want to exclude from the backup plan. **Note** Specify the paths based on the following rules: ◦ You can enter a maximum of eight paths, including paths that include wildcards (*). ◦ If a path does not include forward slashes (/), a wildcard (*) in the path matches multiple directory levels. For example, the *abc* path matches /abc/, /d/eabcd/, and /a/abc and the *.txt path matches all files whose extension is TXT. ◦ If a path includes forward slashes (/), each wildcard (*) in the path matches one directory level. For example, the /a/*/*/share path matches the /a/b/c/share path but does not match the /a/d/share path. ◦ If a path ends with a forward slash (/), the path matches a directory. For example, the *tmp/ path matches the /a/b/aaatmp/ directory and the /tmp/ directory. ◦ The path separator in Linux is the forward slash (/). The path separator in Windows is the backslash (\).

Parameter	Description
Running Plan	The type of the backup plan. Select **Instant**.

4. Optional. Click the **Bandwidth Throttling** tab. Set **Work Hours**. In the Throttling field, enter the maximum bandwidth that can be used for backup during the specified throttling period. Then, click Add.

   > **Note**
   > - The throttling period is accurate to the hour. You can add multiple throttling periods based on your requirements.
   > - If you need to modify a throttling period, find the throttling period, click **Delete** in the Actions column, and then add a throttling period.
   > - The maximum bandwidth must be at least 1 MB/s.

5. Click **Submit**.

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

   - View the progress of the backup job.
   - Click **Cancel** or **Retry** in the Actions column to cancel or retry the backup job.
   - If the backup of some files fail, click the Download icon in the Errors column to download the error report.

Create a scheduled backup plan

If you need scheduled backup, perform the following steps to create a scheduled backup plan:

1. Log on to an HBR backup client.
2. In the left-side navigation pane, click **Backup**.
3. In the upper-right corner of the Backup Jobs page, click **Create Backup** Job.
4. In the **Create Backup Job** dialog box, click the **Basic Settings** tab.
5. Specify the paths to the source files, select **Scheduled** as Running Plan, and then select an existing backup policy as **Backup Policy**.

Parameter	Description

Parameter	Description
Source	The paths to the source files. Specify the paths based on the following rules: ◦ If no wildcard (*) is included, you can enter a maximum of eight source paths. ◦ If wildcards (*) are included, you can enter only one source path. The format of the path can be /*/*. ◦ Only absolute paths are supported. The paths must be start with /, \\, C:\, or D:\. **Note** ◦ If VSS backup is used, you can enter only one path. UNC paths and wildcards (*) are not supported. You cannot specify files to excluded from the backup plan. ◦ If UNC paths are used, VSS backup and wildcards (*) are not supported. You cannot specify files to excluded from the backup plan. If a UNC path is specified, HBR does not back up the access control list (ACL) of Windows.
Use VSS for backup (Windows only)	◦ Specifies whether to use Volume Shadow Copy Service (VSS) for backup. If data in the backup source changes, select this check box. VSS ensures data consistency between the source and the backup. ◦ This parameter is valid only for Windows clients. ◦ If VSS is used, you cannot back up data from multiple directories.

Parameter	Description
Backup Rule	The rule that specifies the files to be excluded from the backup plan. Select **All Files** or **Exclude Files**. If you select **Exclude Files**, specify the paths to files that you want to exclude from the backup plan. **Note** Specify the paths based on the following rules: ◦ You can enter a maximum of eight paths, including paths that include wildcards (*). ◦ If a path does not include forward slashes (/), a wildcard (*) in the path matches multiple directory levels. For example, the *abc* path matches /abc/, /d/eabcd/, and /a/abc and the *.txt path matches all files whose extension is TXT. ◦ If a path includes forward slashes (/), each wildcard (*) in the path matches one directory level. For example, the /a/*/*/share path matches the /a/b/c/share path but does not match the /a/d/share path. ◦ If a path ends with a forward slash (/), the path matches a directory. For example, the *tmp/ path matches the /a/b/aaatmp/ directory and the /tmp/ directory. ◦ The path separator in Linux is the forward slash (/). The path separator in Windows is the backslash (\).
Running Plan	The type of the backup plan. Select **Scheduled**.
Backup Policy	The backup policy. Select an existing backup policy from the drop-down list.

6. Optional. Click the **Bandwidth Throttling** tab. Set **Work Hours**. In the Throttling field, enter the maximum bandwidth that can be used for backup during the specified throttling period. Then, click Add.

> **Note**
> - The throttling period is accurate to the hour. You can add multiple throttling periods based on your requirements.
> - If you need to modify a throttling period, find the throttling period, click **Delete** in the Actions column, and then add a throttling period.
> - The maximum bandwidth must be at least 1 MB/s.

7. Click **Submit**.

   After a backup job is started, you can perform the following operations on the **Backup Jobs** page:
   - View the progress of the backup job.
   - Click **Cancel** or **Retry** in the Actions column to cancel or retry the backup job.
   - Click **Delete** in the Actions column to delete the backup job. After you delete the backup job, HBR no longer runs the backup job based on the specified backup policy. However, HBR retains the backup data of the backup job. You can still restore data from the backup data.
   - If the backup of some files fail, click the Download icon in the Errors column to download the error report.

Query files to be backed up

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

1. On the **File** tab of the On-Premises Backup page, find the backup client, and click **Browse** in the Actions column.
2. On the page that appears, click **Browse** in the Actions column that corresponds to a source path.

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

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

FAQ

If file backup fails due to an unstable network connection, you can perform the following operations and try again:

1. Log on to the ECS instance from which files need to be backed up.
2. Go to the installation directory of the HBR backup client.
3. In the `client` folder, create a file named `hbr.config`.

> **Note** The `hbr.config` file must be in the same directory as the `hybridebackup` and `ids` executable files.

4. Add the following parameters to the `hbr.config` file.

Parameter	Description

Parameter	Description
retry_times	The number of file backup retries. Default value: 3.
retry_interval	The interval at which file backup is retried. Default value: 100 ms.
skip_error_files	Specifies whether to skip files that fail to be backed up. Default value: false. ○ false: does not skip the failed files. ○ true: skips the failed files.

The following script shows example configurations of the parameters in the hbr.config file.

```
retry_times=3
retry_interval=100
skip_error_files=false
```

3.4. Restore files

You can restore files to the source server or virtual machine (VM). You can also restore files to a server or VM that is different from the backup source.

> **Note** If you have a large number of backup files, you can use the file search feature to locate the files that you want to restore. For more information, see Search backups.

Restore files to the source client

To restore files to the source client, perform the following steps:

1. Log on to a Hybrid Backup Recovery (HBR) backup client.
2. In the left-side navigation pane, click **Restore** to open the **Restore Backup / Backups** page.
3. On the **Backups** tab, find the backup, and click **Restore** in the Actions column.
4. In the **Restore Backup** dialog box, set the parameters that are listed in the following table, select the files that you want to restore, and then click **Submit**.

Parameter	Description
Target Folder	The destination folder to which the files are restored.
File Options	○ **Include Files**: Only the selected files and folders are restored to the destination folder. ○ **Exclude Files**: Except for the selected files and folders, all other files and folders are restored to the target folder.

Restore files to a client that is different from the backup source

To restore files to a client that is different from the backup source, perform the following steps:

1. Log on to the destination HBR file backup client.
2. In the left-side navigation pane, click **Restore** to open the **Restore Backup / Backups** page.
3. In the upper-right corner of the Backups tab, click **Restore From Other Client**.
4. In the **Restore Backup** dialog box, select the source client and click **Next**.
5. Select the backup that you want to restore, and click **Next**.
6. In the Restore Backup dialog box, set the parameters that are listed in the following table, select the files that you want to restore, and then click **Submit**.

Parameter	Description
Target Folder	The folder to which the files are restored.
File Options	○ **Include Files**: Only the selected files and folders are restored to the destination folder. ○ **Exclude Files**: Except for the selected files and folders, all other files and folders are restored to the target folder.

3.5. Restore files across regions by using a mirror vault

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

> **Note**
>
> - After a mirror vault is created, backup data in the backup vault is synchronized to the mirror vault in real time. The historical backup data in the backup vault starts to be synchronized to the mirror vault 90 minutes after the mirror vault is created.
> - You can create only one mirror vault for each backup vault.
> - You can restore the backup data that is stored in a mirror vault but cannot back up the data in a mirror vault.
> - You must delete a mirror vault before you can delete the corresponding backup vault.
> - You can create a backup vault when you create a backup client.

Create a mirror vault

To create a mirror vault, perform the following steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, click **Overview**.

3. Find the card of the backup vault for which you want to create a mirror vault. In the upper-right corner of the card, click the

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

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

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

Restore files from a backup stored in a mirror vault

Before you restore files that is stored in a mirror vault, perform the following steps to install a backup client for files on the destination server or virtual machine (VM) and add the client to the mirror vault.

1. Download and install a file backup client on the destination server or VM.

   > **Note** Before you download a backup client, you must create a client. When you create the client, select the mirror vault.

2. Log on to the backup client on the destination server or VM, and restore files from another client.

   > **Note** To find the files that you want to restore, you can use the backup search feature.

3.6. Configure a backup alert

If a backup fails or a backup client is disconnected from Hybrid Backup Recovery (HBR), HBR sends alert notifications to the owner of the Alibaba Cloud account by default. You can configure notification contacts, contact groups, and notification methods.

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

Create a notification contact

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

1. Log on to the HBR console.
2. In the left-side navigation pane, click **Notification Contacts**.
3. On the Notification Contacts page, click the **Contacts** tab.
4. In the upper-right corner, click **Create Contact**.
5. In the **Create Contact** panel, specify the Contact Name parameter.
6. Select **Email** as Notification Methods.

   After you select Email, enter an email address in the **Email** field and click **Send**. Log on to the

specified email box and copy the verification code. Then, paste the code in the Verification Code field in the HBR console.

7. Click **OK**.

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

Create a contact group

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

1. Log on to the HBR console.
2. In the left-side navigation pane, click **Notification Contacts**.
3. On the Notification Contacts page, click the **Groups** tab.
4. In the upper-right corner, click **Create Group**.
5. In the **Create Group** pane, specify a group name.
6. Select the contacts that you want to add to the group and click the > button. Then, the selected contacts are added to the Selected Contacts section.
7. Click **OK**.

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

Create an alert policy

You can create the following types of alert policies:

> **Note** By default, HBR sends alert notifications to the owner of the Alibaba Cloud account by using E-mails.

- Configure an alert policy for a vault

You can configure an alert policy for a vault. The alert policy applies to all the backup clients that are associated with the vault. The backup clients include those used to back up ECS instances, on-premises files, and on-premises virtual machines (VMs). If you do not configure alert policies for the backup clients, the backup clients use the alert policy of the vault by default. To configure an alert policy for a vault, perform the following steps:

i. Log on to the HBR console.
ii. On the **Overview** page, find the vault.
iii. In the upper-right corner of the vault, choose **Settings > Modify Backup Vault** .
iv. In the **Modify Backup Vault** panel, select an alert policy as needed.

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

v. Click **OK**.

- Configure an alert policy for a backup client

  You can configure an alert policy for a backup client. After you create an alert policy for a backup client, the backup client no longer uses the default alert policy, or the alert policy of the associated vault. To configure an alert policy for a backup client, perform the following steps:

  i. Log on to the HBR console.
  ii. In the left-side navigation pane, choose **Backup > On-Premises Backup**.
  iii. On the **File** page, find the client, and choose **More > Alert Settings** in the Actions column.
  iv. In the **Alert Settings** panel, select an alert policy as needed.

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

  v. Click **OK**.

3.7. Use tags

You can use tags to identify resources. Tags allow enterprises and individuals to categorize ECS resources and simplify the search and management of resources. This topic describes how to use the tagging feature to back up files from on-premises clients.

Prerequisites

Authorization is completed in Resource Access Management (RAM) and a file backup client is installed. For more information, see Preparations.

Context

You can create different tags for different on-premises clients. For example, if you manage teams or projects, you can create tags based on department or project and use these tags to categorize your instances. For example, you can create a tag named `project:a` for a project. This way, you can filter on-premises clients based on the tag when you maintain your on-premises clients.

Usage notes

- Each tag consists of a key-value pair.
- A tag must be unique.

  For example, the `company:a` tag is added to a backup vault. If you add the `company:b` tag to the backup vault, the company:a tag is replaced with the `company:b` tag.
- Tags are not shared across regions. For example, tags that are created in the China (Hangzhou) region are invisible to the China (Shanghai) region.

Limits

When you create tags, take note of the following limits:

Item	Limit
The maximum length of a key	128 characters
The maximum length of a value	128 characters
The maximum number of custom tags that you can add to a resource	20
The key of a tag	• The key cannot start with `aliyun` or `acs:`. • The key cannot contain `http://` or `https://`. • The key cannot be an empty string.
The value of a tag	A tag value cannot contain `http://` or `https://`.

Create tags

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > On-Premises Backup**.

3. In the top navigation bar, select a region.
4. On the **On-Premises Backup** page, click **File**.
5. In the **Tags** column next to the name or ID of the on-premises client, click the icon.
6. In the dialog box that appears, click **Edit**.
7. In the **Key** and **Value** fields, enter the key-value pair of a tag and click **Save**.

   If you want to create more than one tags, click **Add a row** to specify the key-value pair of a new tag.

Search for a resource by tag

In the upper-right corner of the **File** tab, select **Tags** from the drop-down list and enter the tag information. Then, click the **Search** icon.

- You can search for a resource by using a key, as shown in the following example:

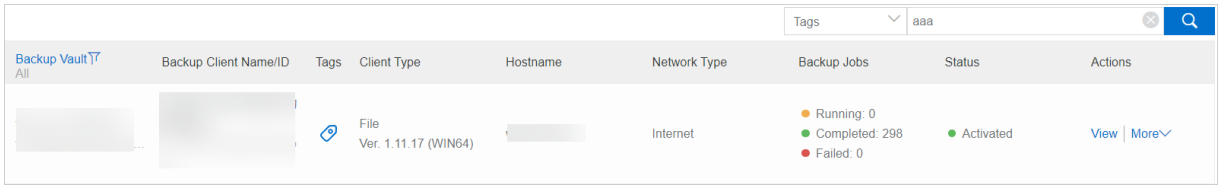
  ```
  aaa
  ```

- You can search for a resource by using a key-value pair, as shown in the following example:

  ```
  aaa:bbb
  ```

- You can search for a resource by using multiple key-value pairs, as shown in the following example:

  ```
  aaa:bbb,ccc:ddd
  ```



4.VMware VM backup

4.1. Overview

Hybrid Backup Recovery (HBR) is a fully managed online backup service that allows you to back up data to the cloud in an efficient, secure, and cost-effective way. You can use HBR backup client to back up images of on-premises VMware virtual machines (VMs). You can then restore the VMs if needed.

You can use the following procedure to back up a VMware VM:

- Prepare for backup
- Back up VMware VM images
- Restore VMware VMs from images

For information about other features of on-premises VMware VM backup, see the following topic:

Configure alert notifications

4.2. Prepare for a data backup

You can use Hybrid Backup Recovery (HBR) to back up the images of on-premises VMware vSphere virtual machines (VMs). You can restore VMs from the images based on your business requirements. This topic describes how to prepare for a data backup.

(Recommended) Prepare an AccessKey pair for a RAM user

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

An AccessKey pair is required when you activate a backup client. The AccessKey pair is an identity credential. If an AccessKey pair of your Alibaba Cloud account is used, all cloud resources that belong to the account are exposed to risks. Therefore, we recommend that you use an AccessKey pair of a RAM user to activate backup clients. Before you back up data, make sure that a RAM user is created and an AccessKey pair is created for the RAM user. For more information, see Create a RAM user and Create an AccessKey pair for a RAM user.

Step 1: Create a backup client

Before you back up and restore the images of VMs, you must install a backup client on the server on which the vSphere Client is deployed. To create a backup client in the HBR console and download the template of the client, perform the following steps:

1. On the server on which the vSphere Client is deployed, log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > On-Premises Backup**.
3. On the left of the top navigation bar, select a region.
4. On the **On-Premises Backup** page, click **VMware VM**.
5. In the upper-right corner of the On-Premises Backup page, click **Add Client**.
6. In the **Add Client** panel, configure the parameters and click **Create**.

   The following table describes the parameters.

Parameter	Description
Vault Name	The backup vault to which you want to store backup data. A backup vault is a repository that HBR uses to store backup data. You can use a single vault to store backup data that is received from multiple backup clients. ○ One or more backup vaults exist. Select a backup vault from the Vault Name drop-down list. ○ No backup vault exists. Click **Create Vault**. Enter a name for the new backup vault in the **Vault Name** field. The name must be 1 to 64 characters in length.
Client Name	The name of the backup client. The name must be 1 to 64 characters in length.
Software Platform	The software platform of the VM from which you want to back up data. Default value: vSphere.
Network Type	○ **Virtual Private Cloud (VPC)**: If the server or VM from which you want to back up data resides in a VPC and the VPC is in the same region as the backup vault, select this option. **Note** VM backup clients are connected to VPCs by using routes. You can use a VM backup client to access the IP addresses in the following Classless Inter-Domain Routing (CIDR) blocks of VPCs from an on-premises VM: 100.64.0.0/10, 100.64.0.0/11, and 100.96.0.0/11. ○ **Internet**: If no VPCs are available, select this option.
Use HTTPS	Specifies whether to use HTTPS to transmit encrypted data that is stored in a backup vault. HTTPS reduces the performance of data transmission. If you modify the setting of this switch, the modification takes effect on the next backup or restore job.

7. In the **Add Client** panel, click **Download Client** and **Download Certificate**.

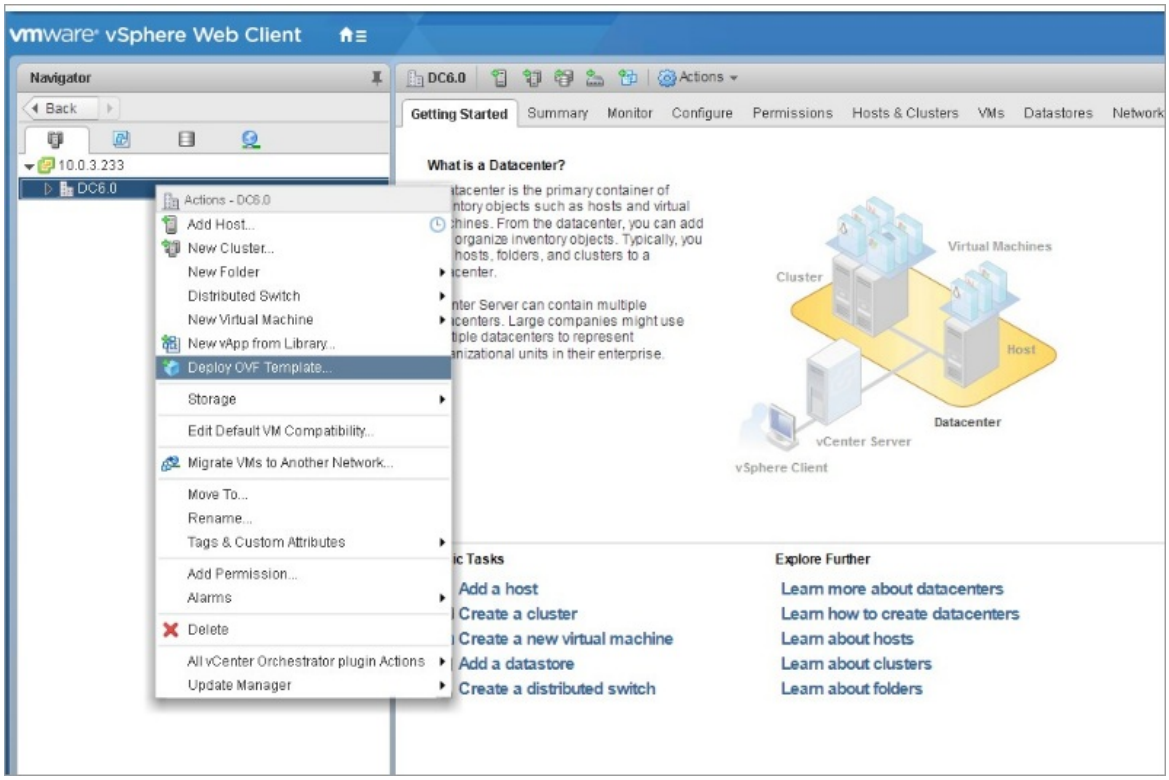
Note The backup client is used to connect your VM to HBR, and the certificate is used to activate the client. You can also download the client and the certificate from the client list.

Step 2: Install the backup client

After you download the client and the certificate, install the client on the VM. You can use the client to back up VM images and restore VMs from images. To install the client, perform the following steps:

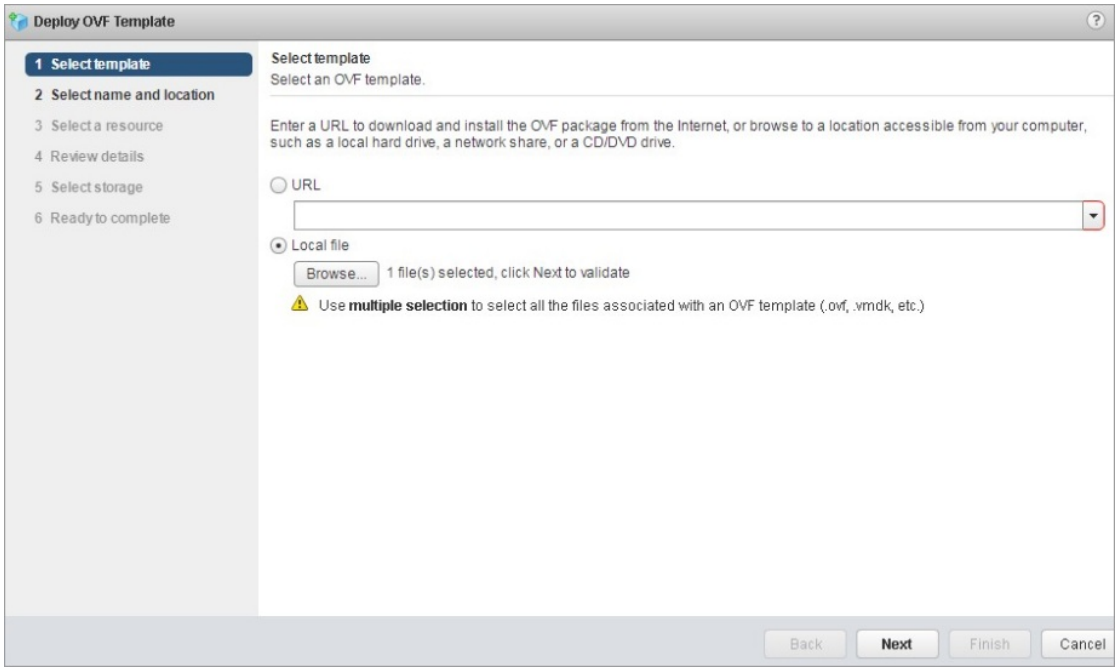
1. Log on to the vSphere Web Client.
   - HBR supports only vCenter Server 5.5, 6.0, 6.5, 6.7, and 7.0.
   - You can use a browser to log on to the Flash-based or HTML5-based vSphere Web Client.

2. In the left-side navigation pane, right-click the VM and select **Deploy OVF Template** from the shortcut menu.



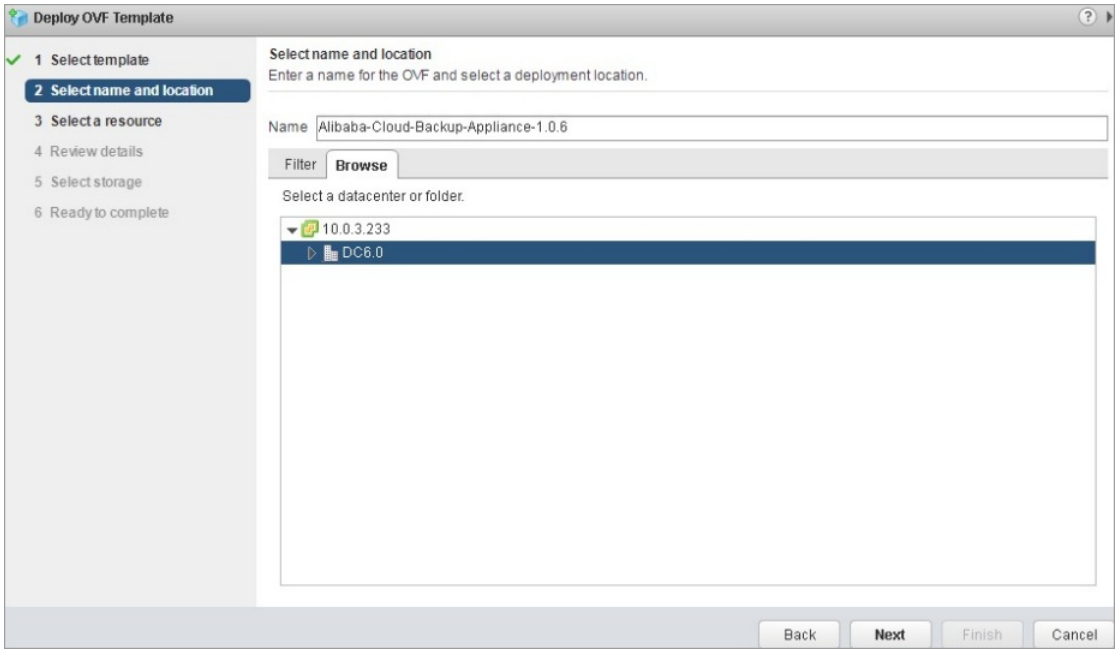
For more information, see Deploying OVF and OVA Templates.

i. In the **Deploy OVF Template** dialog box, select **Local file**. Click **Browse**, select the client template that you downloaded, and then click **Next**.

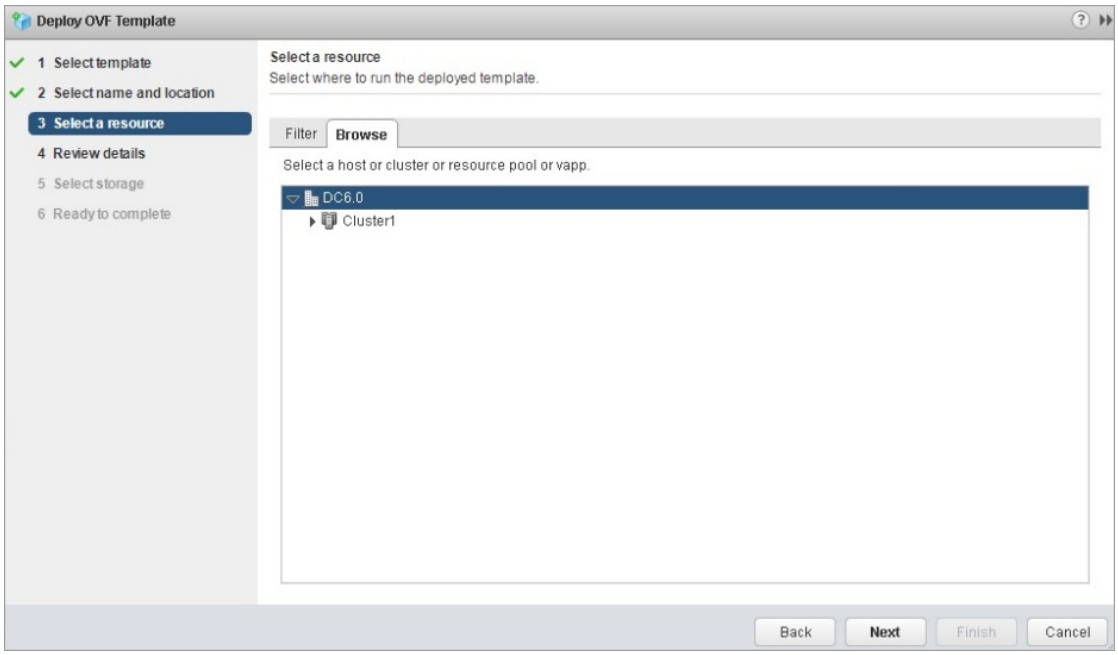


> **Note** To reduce the download time, HBR provides a client package in the open virtual appliance (OVA) format. You can use the client package to deploy OVA templates on the vSphere Web Client.

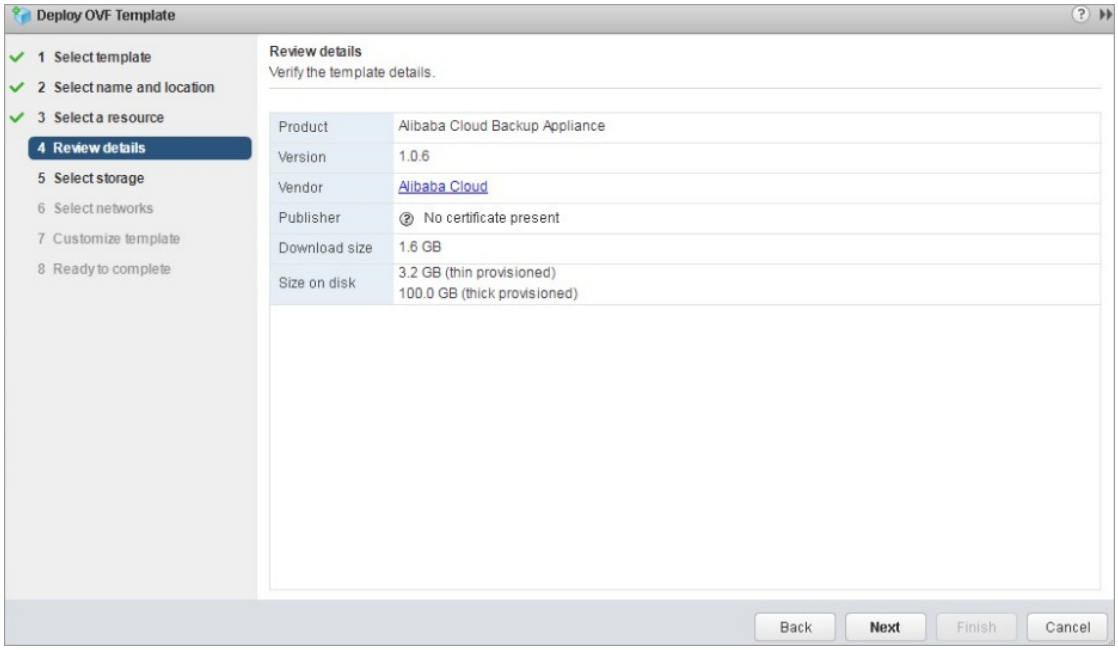
ii. Enter the name of the open virtual format (OVF) template or OVA template, select the location where you want to deploy the template, and then click **Next**.



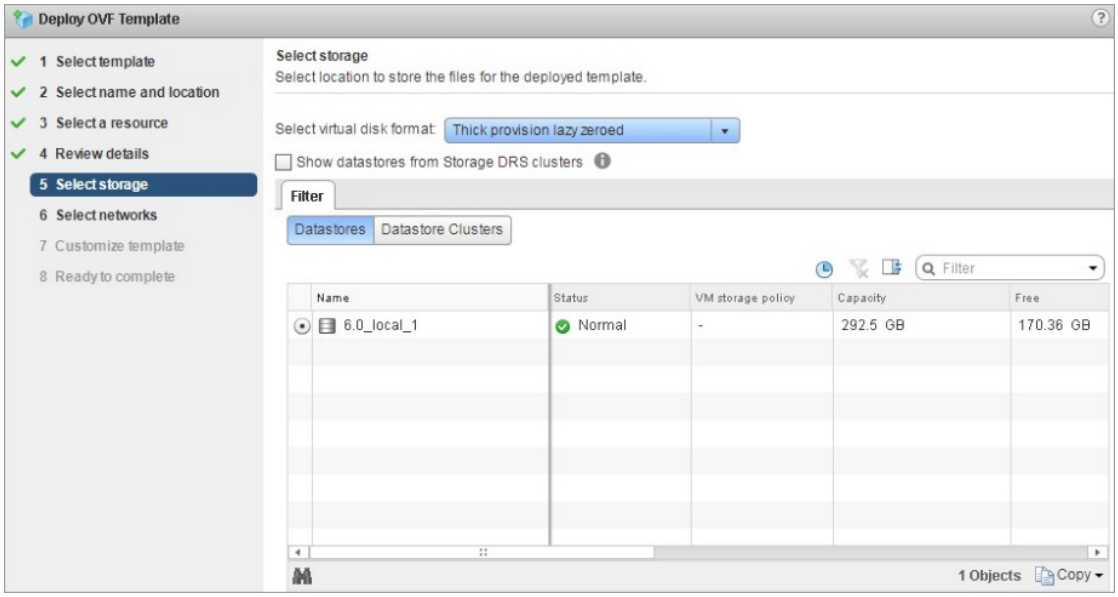
iii. Select the location where you want to run the deployed template and click **Next**.



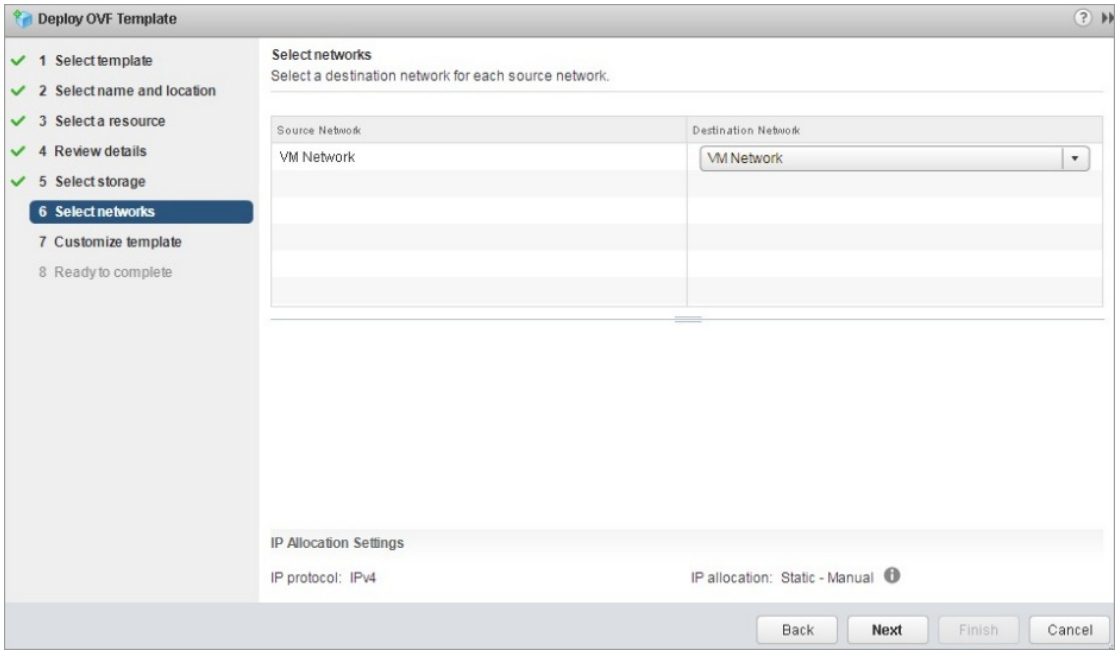
iv. Verify the information about the template and click **Next**.



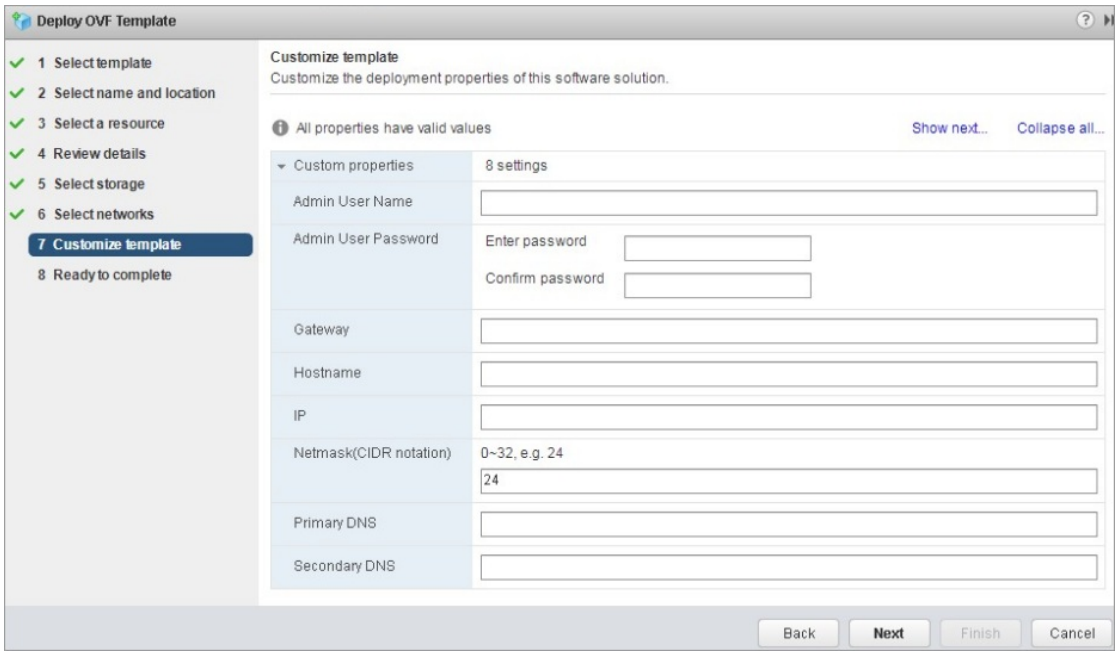
v. Select the format of the virtual disk based on your business requirements, select a storage resource to which you want to store the files of the template that you deployed, and then click **Next**.



vi. Select a destination network for each source network and click **Next**.

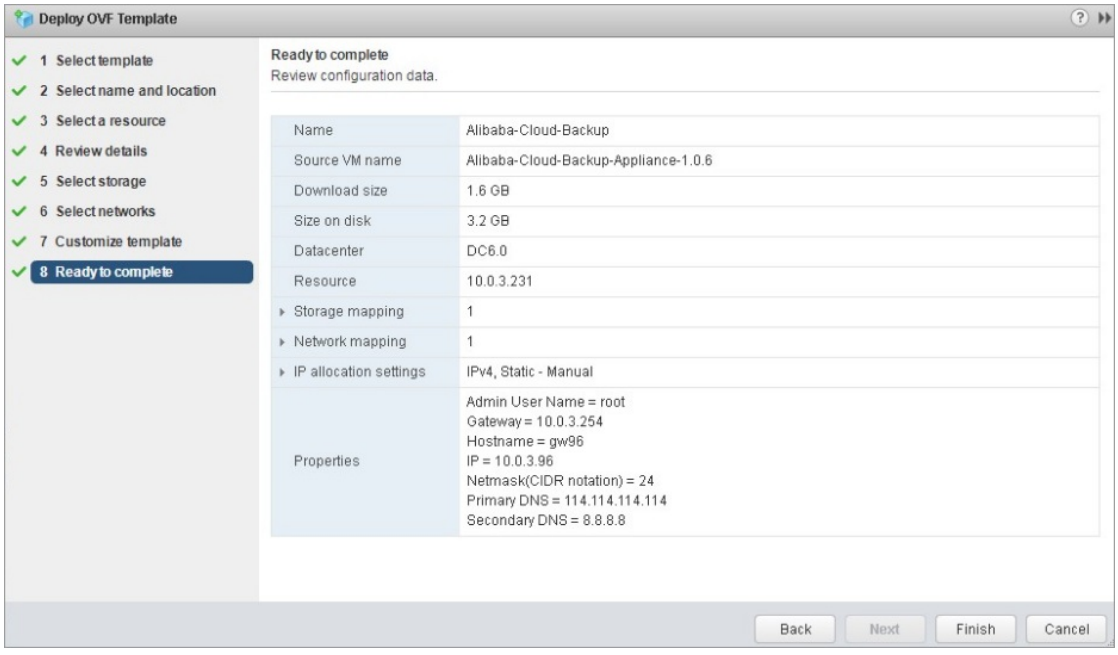


vii. Configure the required deployment properties for the software solution and click **Next**.

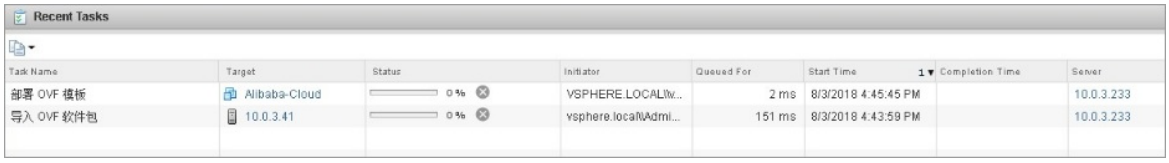


> **Note** Enter a reachable IP address of the VPC that you want to access. If no domain name server (DNS) for mapping domain names to VPC endpoints is available on your host, enter the server IP address of Alibaba Cloud DNS PrivateZone, for example, 100.100.2.136 or 100.100.2.138.

viii. Verify the configurations and click **Finish**.



3. View the progress of each deployment task in the Recent Tasks section.



4. After the deployment tasks are complete, start the VM on which the OVF or OVA template is deployed.
5. Open a browser, and enter `http://hostname:8011` in the address bar.

   Replace the `hostname` with the IP address of the VM on which the OVF or OVA template is deployed.
6. On the **Register** page, configure the parameters and click **Register** to log on to the HBR gateway. The following table describes the parameters.

Parameter	Description
AccessKey ID	The AccessKey ID and AccessKey secret of the RAM user that is used to access HBR. You can obtain the AccessKey ID and AccessKey secret of a RAM user from your Alibaba Cloud account for which HBR is activated. For more information, see How can I create an AccessKey pair for a RAM user?.
AccessKey Secret	
Password	The password that is used to log on to the backup client. The password must be at least six characters in length.
Certificate File	The certificate that you downloaded from the HBR console. If a VM is shut down for more than five days after you use the certificate to activate the client on the VM, the certificate expires. You must download a new certificate and reactivate the client.

FAQ

- Why am I unable to upload an OVA template?

  You may be unable to upload an OVA template because the vCenter Server version of the vSphere Web Client is not supported, the browser is not supported by the vCenter Server, or the language of the browser is not supported. Perform the following steps to troubleshoot the error:

  - Check whether the vCenter Server version of the vSphere Web Client is supported by HBR. Only the following vCenter Server versions are supported: 5.5, 6.0, 6.5, 6.7, or 7.0.
  - If you use vCenter Server 6.0, use an earlier version of Firefox, for example, Firefox 38.0, to deploy the OVA template.
  - If a message appears to remind you of a common error when you deploy an OVA template, we recommend that you change the language of your browser to English and then deploy the OVA template again.
- Why am I unable to add a vCenter Server instance to the HBR gateway even if the IP address, username, and password are correct?

A vCenter Server may fail to be added if the password contains the following special characters:

` ^ ~ = ; ! / ([ ] { } @ $ \ & # % +

> **Note** We recommend that you create a vCenter Server account that is dedicated for backup. We recommend that you use periods (.) instead of other special characters in the password of the account.

What's next

Back up VMware VM images

4.3. Back up VMware VM images

This topic describes how to back up the images of VMware virtual machines (VMs). Hybrid Backup Recovery (HBR) provides two types of backup plans for on-premises VMware VMs: instant and scheduled. HBR also supports incremental backup for scheduled backup plans. This improves data security.

Prerequisites

The preparations for VMware VM backup are completed. For more information, see Prepare for a data backup.

Step 1: Add a vCenter Server

Before you back up on-premises VMware VMs, you must add a vCenter Server in the HBR console.

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > On-Premises Backup**.
3. In the top navigation bar, select the region where the VMware Server resides.
4. On the **On-Premises Backup** page, click **VMware VM**.
5. Click the **Managed vCenter Servers** tab. In the upper-right corner of the tab, click **Add vCenter Server**.
6. In the **Add vCenter Server** panel, set the **Server IP**, **Username**, **Password**, and **Description** parameters. The Description parameter is optional. Then, click **Create**.

   A vCenter Server may fail to be added if the password contains the following special characters:

   ` ^ ~ = ; ! / ([ ] { } @ $ \ & # % +

   > **Note** We recommend that you create a vCenter Server account that is dedicated for backup. We recommend that you use periods (.) instead of other special characters in the password of the account.

Step 2: Create a backup plan

To create a backup plan, perform the following steps:

1. On the vCenter Servers tab, click **Create Backup Plan** in the Actions column next to the added vCenter Server.
2. In the Create Backup Plan dialog box, set the parameters in the **Config Backup Plan** step and click **Next**. The following table describes the parameters.

Parameter	Description
Plan Name	The name of the backup plan. If you do not specify a value for this parameter, a random name is generated for the backup plan.
Retention	The retention period of backup data. Unit: days, weeks, months, or years.
Force Silent Snapshot	Specifies whether to forcibly use silent snapshots. ◦ If you select this check box, HBR uses silent snapshots to back up data. If no silent snapshots are created, the backup fails. ◦ If you do not select this check box, HBR attempts to use silent snapshots to back up data. If no silent snapshots are created, HBR uses common snapshots to back up data. By default, this check box is not selected.
Use Lan-Free	Specifies whether to perform a LAN-free backup. If you select this check box, the disk that you want to back up is mounted on the HBR gateway, and data is transferred over a storage area network (SAN) instead of a local area network (LAN). If the mount fails, data is transferred over a LAN.
Backup Policy	The policy that is used to back up data. Valid values: **Instant Backup** and **Schedule Backup**. If you click **Schedule Backup**, you must specify the **Start Time**, **Plan Interval**, and **Incremental Backup Policy** parameters for the scheduled backup plan. If you enable incremental backup, you must specify the **Start Time** and **Plan Interval** parameters for incremental backup. **Notice** ◦ If the Changed Block Tracking (CBT) feature is disabled for a VM, a full backup is performed instead of an incremental backup. For more information about CBT, see the VMware documentation. ◦ Incremental backup includes only the data that is generated or modified after the most recent full or incremental backup job is completed. ◦ We recommend that you perform a full backup at least 1 hour after the previous incremental backup is completed.
Start Time	If the **Backup Policy** parameter is set to **Schedule Backup**, you must set this parameter. This parameter specifies the time at which the backup starts. You can set this parameter based on your backup plan. The default value is the time when the backup plan is created.

Parameter	Description
Plan Interval	If the **Backup Policy** parameter is set to **Schedule Backup**, you must set this parameter. Select the interval at which backups are performed. Default value: 1. Unit: hours, days, or weeks.
Incremental Backup Policy	If the **Backup Policy** parameter is set to **Schedule Backup**, you must set this parameter. This parameter specifies whether to enable incremental backup. Valid values: ○ No: Disable incremental backup. Default value: No. ○ Yes: Enable incremental backup.

3. In the **VM to Backup** step, select the source VM and click **Next**.
4. In the **Confirm & Execute** step, check whether the backup plan is configured based on your business requirements. The configurations include the backup plan name, retention period, backup policy, and VMs. Then, click **Create**.

   After the backup plan is created, HBR runs backup jobs based on the backup plan. On the **Backup Plans** tab, you can perform the following operations:

   - To start a backup job, find the backup plan that you want to run and click **Run Now** in the Actions column.
   - To suspend a running backup job, find the backup plan that you want to suspend and choose **More > Suspend Plan** in the Actions column. To resume a suspended backup job, find the backup plan that you want to resume and choose **More > Resume Plan** in the Actions column.
   - To delete a backup plan, find the backup plan that you want to delete and choose **More > Delete Plan** in the Actions column. After you delete a backup plan, HBR no longer runs the backup plan. However, the backup data is still retained.

Specify a backup client

After a backup plan is created, backup jobs are dispatched to backup clients based on the real-time client status. The client status includes the number of jobs that are running on each client, whether LAN-free backup is enabled for each client, and the performance of the ESXi host of each VM.

If you need to back up a large number of VMs, you can install multiple backup clients to increase backup efficiency. The procedure to install multiple backup clients is similar to the procedure to install a single backup client. For more information, see Prepare for a data backup.

After multiple backup clients are installed, HBR schedules backup jobs based on the client status, which includes the load of each backup client. You can also specify a backup client on which you want to run a backup plan.

1. Log on to the HBR console.
2. In the top navigation bar, select the region where the VMware VM resides.
3. In the left-side navigation pane, choose **Backup > On-Premises Backup**.
4. On the **On-Premises Backup** page, click **VMware VM**.
5. Click the **Backup Plans** tab. On the Backup Plans tab, find the backup plan for which you want to specify a backup client, and choose **More > Designate Client** in the Actions column.
6. In the **Designate Client** panel, select the backup client on which you want to run the backup plan.

7. Click **Create**.
   On the **Backups** tab, the information about backup jobs is displayed. The information includes the backup clients that run the backup jobs on a VMware VM.

References

- For more information about how to restore a VMware VM to an on-premises vCenter Server, see Restore VMware VMs from images to an on-premises vCenter Server.
- For more information about how to restore a VMware VM to an Alibaba Cloud ECS instance, see Restore a VMware VM to an ECS instance.
- For more information about how to use the instant mount feature of HBR to restore specified files on a VMware VM to an Alibaba Cloud ECS instance, see Restore specified files on a VMware VM to an ECS instance.

What's next

Restore VMware VMs from images to an on-premises vCenter Server

4.4. Restore VMware VMs from images to an on-premises vCenter Server

This topic describes how to restore VMware virtual machines (VMs) from images to an on-premises vCenter Server in the Hybrid Backup Recovery (HBR) console.

Prerequisites

A VMware VM is backed up. For more information, see Back up VMware VM images.

Context

- Alibaba Cloud continually updates Hybrid Backup Recovery to support more regions. You can log on to the HBR console to view the supported regions.
- After you back up the image of a VMware VM, you can use the HBR console to restore the image to an on-premises vCenter Server in the case of VMware VM failure to ensure business continuity.
- The on-premises VMware VM backup feature of HBR 1.0.13 and later versions allow you to manage backup and restore jobs in the HBR console. If you have configured on-premises backup plans, re-configure them in the HBR console.

Procedure

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > On-Premises Backup**.
3. In the top navigation bar, select the region where the VMware VM resides.
4. On the **On-Premises Backup** page, click **VMware VM**.
5. Click the **Backups** tab.
6. On the Backups tab, find the backup plan and click **Restore** in the **Actions** column.
7. In the **Create Restore Job** panel, set the parameters in the **Virtual Machine**, **Location**, **Computer**, **Storage** , **Network**, and **Confirm and Execute** steps. After you set the parameters, click **Create**.
   After the restore job is created, you can view information of the job on the **Restore Jobs** tab. The

information includes the status of the job and the volume of data that is restored.

4.5. Collect logs and diagnose network issues

This topic describes how to collect logs and diagnose the network issues of VMware virtual machine (VM) backup clients. You can collect logs regardless of whether you have logged on to the Hybrid Backup Recovery (HBR) gateway or not.

Prerequisites

The preparations for VMware VM backup are completed. For more information, see Prepare for a data backup.

Context

- You can use the log collection feature to collect the logs of VMware VM backup clients. You can analyze the logs to identify issues. This feature improves the operations and maintenance efficiency.
- You can use the network diagnosis feature to check network connections in real time and identify and fix network issues at the earliest opportunity.

Collect the logs of a VMware VM backup client

You can collect the logs of a backup client, regardless of whether you have logged on to the HBR gateway or not.

- Collect logs when you have not logged on to the HBR gateway

  To collect the logs of a backup client when you have not logged on to the HBR gateway, perform the following steps:

  i. Open a browser, enter the logon address of the backup client `http://hostname:8011` in the address bar, and then press Enter.
  ii. In the upper-left corner of the logon page, click **Diagnose**.
  iii. In the dialog box that appears, choose **Collect Logs > Download Logs**.

- Collect logs when you have logged on to the HBR gateway

  To collect the logs of a backup client when you have logged on to the HBR gateway, perform the following steps:

  i. In the upper-right corner of the logon page, click the icon next to admin, and select **Diagnose** from the shortcut menu.
  ii. In the dialog box that appears, choose **Collect Logs > Download Logs**.

Diagnose the network issues of a VMware VM backup client

You can diagnose the network issues of a backup client, regardless of whether you have logged on to the HBR gateway or not.

- Diagnose network issues when you have not logged on to the HBR gateway

  To diagnose the network issues of a backup client when you have not logged on to the HBR gateway, perform the following steps:

i. Open a browser, enter the logon address of the backup client `http://hostname:8011` in the address bar, and then press Enter.
ii. In the upper-left corner of the logon page, click **Diagnose**.
iii. In the dialog box that appears, choose **Network Diagnosis > Start Detection**.

- Diagnose network issues when you have logged on to the HBR gateway

  To diagnose the network issues of a backup client when you have logged on to the HBR gateway, perform the following steps:

  i. In the upper-right corner of the logon page, click the icon next to admin, and select **Diagnose** from the shortcut menu.
  ii. In the dialog box that appears, choose **Network Diagnosis > Start Detection**.

4.6. Configure alert notifications

By default, if a backup attempt fails or a backup client is disconnected from the server, Hybrid Backup Recovery (HBR) sends alert notifications to the owner of the Alibaba Cloud account by using emails. You can specify notification contacts, contact groups, and notification methods.

Prerequisites

A VMware virtual machine (VM) is backed up. For more information, see Back up VMware VM images.

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

Create a notification contact

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

1. Log on to the HBR console.
2. In the left-side navigation pane, click **Notification Contacts**.
3. On the Notification Contacts page, click the **Contacts** tab.
4. In the upper-right corner, click **Create Contact**.
5. In the **Create Contact** panel, enter a contact name.
6. Set the Notification Methods parameter to **Email** and click **OK**.

   After you select Email, enter an email address in the **Email** field and click **Send**. Log on to the account of the specified email address and copy the verification code from the received email. Then, paste the code in the Verification Code field in the HBR console.

> **Note**
> - 在**报警联系人管理**页面，您可以看到所有的报警联系人及其相关信息。
> - 您可以单击**编辑**，修改联系人的邮箱。
> - 已被选定为报警通知，或已经加入其它报警联系组的联系人不可删除。

Create a contact group

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

1. In the left-side navigation pane, click **Notification Contacts**.
2. On the Notification Contacts page, click the **Groups** tab.
3. In the upper-right corner of the tab, click **Create Group**.
4. In the **Create Group** panel, enter a group name.
5. Select the contacts that you want to add to the group and click the > button. Then, the selected contacts are added to the Selected Contacts section. Click **OK**.

> **Note**
> - On the **Groups** tab, you can view information about all created contact groups and the number of contacts in each group.
> - You can click **Modify** to modify a contact group.
> - If a group is specified to receive alert notifications, you cannot delete the contact group.

Create an alert policy

You can configure an alert policy for a vault in the HBR console.

> **Note** By default, if you do not configure an alert policy for a vault, HBR sends alert notifications to the owner of the Alibaba Cloud account by using emails.

1. On the **Overview** page, find the vault for which you want to configure an alert policy.
2. In the upper-right corner of the vault card, choose **Settings > Modify Backup Vault** .
3. In the **Modify Backup Vault** panel, select an alert policy based on your business requirements and click **OK**.

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