ALIBABA CLOUD

Alibaba Cloud

Hybrid Backup
Best Practices

Document Version: 20220602

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.Create a RAM user and grant permissions to the RAM user

After you create a RAM user and grant the required permissions to the RAM user, you can use the RAM user to manage Hybrid Backup Recovery (HBR) resources. This reduces the security risks for your Alibaba Cloud account. This topic describes how to create a RAM user and how to grant permissions to the RAM user.

Context

In actual scenarios, you may need to perform O&M operations on HBR or access HBR resources as a RAM user. In the preceding scenarios, you can create a RAM user and grant the RAM user the permissions to access or manage HBR resources. To ensure data security, we recommend that you follow the principle of least privilege (PoLP) when you grant permissions to the RAM user. For more information about RAM users, see Introduction.

Step 1: Create a RAM user

To manage user permissions by using Resource Access Management (RAM), you must first create RAM users. Then, you must grant different permissions to each RAM user.

If you have multiple RAM users within your Alibaba Cloud account, you can create RAM user groups to classify and authorize these RAM users. This way, you can manage RAM users and permissions with high efficiency. For more information, see Create a RAM user.

To create a RAM user, perform the following steps:

1. Log on to the RAM console by using your Alibaba Cloud account.
2. In the left-side navigation pane, choose **Identities > Users**.
3. On the **Users** page, click **Create User**.
4. In the **User Account Information** section of the **Create User** page, configure the **Logon Name** and **Display Name** parameters.

   > ⓘ **Note** You can click **Add User** to create multiple RAM users at a time.

5. In the **Access Mode** section, select an access mode.
   - **Console Access**: If you select this option, you must complete the logon security settings. These settings specify whether to use a system-generated or custom logon password, whether the password must be reset upon the next logon, and whether to enable multi-factor authentication (MFA).

     > ⓘ **Note** If you select Custom Logon Password in the Console Password section, you must specify a password. The password must meet the complexity requirements. For more information about the complexity requirements, see Configure a password policy for RAM users.

   - **OpenAPI Access**: If you select this option, an AccessKey pair is automatically created for the RAM user. The RAM user can call API operations or use other development tools to access Alibaba Cloud resources.

> ? **Note** To ensure the security of the Alibaba Cloud account, we recommend that you select only one access mode for the RAM user. This prevents the RAM user from using an AccessKey pair to access Alibaba Cloud resources after the RAM user leaves the organization.

6. Click **OK**.

Step 2: Grant permissions to the RAM user

By default, a new RAM user has no permissions. Before you can use the RAM user to perform operations in the HBR console or call API operations, you must grant the required permissions to the RAM user.

provides two system policies:

- AliyunHbrFullAccess: grants a RAM user the full access permissions on HBR.
- AliyunHbrReadOnlyAccess: grants a RAM user the read-only permissions on HBR.

You can also attach custom policies to the RAM user in the RAM console to achieve fine-grained access control. For more information, see Create a custom policy

In this example, the AliyunLogReadOnlyAccess policy is attached to a RAM user.

1.
2.
3.
4.
5. In the **Add Permissions** panel, go to the Select Policy section. Select **System Policy**, enter **AliyunHbrReadOnlyAccess** in the search box, and then press Enter. Click AliyunHbrReadOnlyAccess to add the policy to the Selected section, and then click **OK**.

   > ? **Note** In the Selected section on the right, you can click the cross sign (×) next to a policy to remove the policy.

6. Confirm the authorization result and click **Complete**.

What to do next

You can grant a RAM user the permissions on a backup vault. The permissions allow the RAM user only to back up or restore the backup vault.

You can grant permissions by using the following sample policies. To create a custom policy, copy one of the scripts and paste the script in the RAM console. Then, attach the custom policy to the RAM user. For more information, see Isolate backup permissions and recovery permissions.

- To disable the restore feature for a RAM user, use the following sample policy:

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "hbr:CreateRestore",
                "hbr:CreateRestoreJob",
                "hbr:CreateHanaRestore",
                "hbr:CreateUniRestorePlan",
                "hbr:CreateSqlServerRestore"
            ],
            "Resource": [
                "acs:hbr:*:1178******531:vault/v-000******blx06",
                "acs:hbr:*:1178******531:vault/v-000******blx06/client/*"
            ]
        }
    ]
}
```

- To disable the backup feature for a RAM user, use the following sample policy:

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "hbr:CreateUniBackupPlan",
                "hbr:UpdateUniBackupPlan",
                "hbr:DeleteUniBackupPlan",
                "hbr:CreateHanaInstance",
                "hbr:UpdateHanaInstance",
                "hbr:DeleteHanaInstance",
                "hbr:CreateHanaBackupPlan",
                "hbr:UpdateHanaBackupPlan",
                "hbr:DeleteHanaBackupPlan",
                "hbr:CreateClient",
                "hbr:CreateClients",
                "hbr:UpdateClient",
                "hbr:UpdateClientSettings",
                "hbr:UpdateClientAlertConfig",
                "hbr:DeleteClient",
                "hbr:DeleteClients",
                "hbr:CreateJob",
                "hbr:UpdateJob",
                "hbr:CreateBackupPlan",
                "hbr:UpdateBackupPlan",
                "hbr:ExecuteBackupPlan",
                "hbr:DeleteBackupPlan",
                "hbr:CreateBackupJob",
                "hbr:CreatePlan",
                "hbr:UpdatePlan",
                "hbr:CreateTrialBackupPlan",
                "hbr:ConvertToPostPaidInstance",
                "hbr:KeepAfterTrialExpiration"
            ],
            "Resource": [
                "acs:hbr:*:1178******9531:vault/v-000******blx06",
                "acs:hbr:*:1178******9531:vault/v-000******blx06/client/*"
            ]
        }
    ]
}
```

What's next

Use a RAM user to log on to the RAM console

2.Back up files from a local server that is not connected to the Internet

Before you back up files from a local server that is not connected to the Internet, you must connect the server to a virtual private cloud (VPC) by using a VPN gateway or an Express Connect circuit. Then, you can create a configuration file named *hybridbackup.toml* to back up files from the server. This topic describes how to create and configure the *hybridbackup.toml* configuration file.

Prerequisites

- The local server resides in the China (Beijing), China (Shanghai), China (Hangzhou), or China (Shenzhen) region. The local server is connected to a VPC by using a VPN gateway or an Express Connect circuit.
- A backup client is installed. You do not need to activate the backup client. For more information, see Prepare for a data backup.
- A VPN gateway is created. If you want to use a VPN gateway to connect the local server to a VPC, you must create the VPN gateway. For more information, see Create and manage a VPN gateway.

Procedure

1. Create a configuration file.
   - If the backup client runs on Windows, perform the following steps:
     a. Go to the *client* directory in the installation directory of the backup client.

     > Note
     >
     > - By default, the installation path for a backup client of version 1.x is *C:\Program Files\Aliyun Hybrid Backup Service*.
     > - By default, the installation path for a backup client of version 2.x is *C:\Program Files\Aliyun Hybrid Backup Service Client*. We recommend that you use an Express Connect circuit to connect your local server to a VPC. In **Client Settings**, the **Network** parameter must be set to **VPC**.

     b. Create a configuration file named *hybridbackup.toml*.

     c. Add the following information to the *hybridbackup.toml* file and save the file:

     > Notice Replace cn-hangzhou with the ID of the region where the local server resides.

     ```
     [Server]
     Endpoint = "hbr-vpc.cn-hangzhou.aliyuncs.com"
     ```

   - If the backup client runs on Linux, perform the following steps:

a. Go to the *client* directory in the installation directory of the backup client.

> Note
>
> - The default installation path for a backup client of version 1.x is */opt/alibabacloud/hbr*.
> - The default installation path for a backup client of version 2.x is */opt/alibabacloud/hbrclient*. We recommend that you use an Express Connect circuit to connect your local server to a VPC. In **Client Settings**, the **Network** parameter must be set to **VPC**.

b. Create a configuration file named *hybridbackup.toml*.

```
vi /opt/alibabacloud/hbr/client/hybridbackup.toml
```

c. Add the following information to the *hybridbackup.toml* file and save the file:

> Notice Replace cn-hangzhou with the ID of the region where the local server resides.

```
[Server]
Endpoint = "hbr-vpc.cn-hangzhou.aliyuncs.com"
```

2. Restart the Hybrid Backup Recovery (HBR) service.

   - Windows backup client

     Open the Command Prompt, enter **services.msc**, and then press Enter. In the Services dialog box, find and restart the HBR service.

   - Linux backup client

     Run the following command to restart the HBR service:

```
# Restart the HBR service in Linux version 2.x.
systemctl restart hbrclient
restart hbrclient
/etc/init.d/hbrclient restart
# Restart the HBR service in Linux version 1.x.
systemctl restart hybridbackup
restart hybridbackup
/etc/init.d/hybridbackup restart
```

3.Use a cache to accelerate the data backup process

The cache feature is enabled by default on a Hybrid Backup Recovery (HBR) client. You can use a cache to accelerate the data backup process. However, you cannot use the cache to help restore data on a local or remote host. This topic describes how to optimize the settings of a cache.

Prerequisites

An HBR client is installed for local files. The version of the client is 1.5.0 or later. For more information, see Prepare for a data backup.

Context

The cache feature allows you to accelerate the data backup process by caching data entry IDs and metadata. The feature reduces network requests during data backup. You can disable this feature or optimize its settings on the backup source.

Procedure

You can perform the following steps to create a cache configuration file. You can also disable the cache feature or optimize its settings by using the configuration file. This file is optional. If you do not create a file, the default settings of the feature are used. The backup process is not affected.

1. Log on to the on-premises server or virtual machine (VM) whose files you want to back up.
2. Open the installation folder of the HBR client.

   You can find the installation path based on the following default installation paths.

   - For backup clients of an earlier version

     Linux: */opt/alibabacloud/hbr*

     Windows: *C:\Program Files\Aliyun Hybrid Backup Service*

   - Backup clients of the latest version

     Linux: */opt/alibabacloud/hbrclient*

     Windows: *C:\Program Files\Aliyun Hybrid Backup Service Client*

3. In a subdirectory of the *client* folder, create a file named `hbr.config`, and add the information of the data entry ID and metadata cache to the file.

   > **Note** The *hbr.config* file must be at the same directory level as the *ids* file.

   The following example shows the configurations of the *hbr.config* file:

   ```
   disable_blob_cache = false
   max_blob_cache_weight = 0.15
   cache_prefix = D:\CacheFolder
   max_retain_count = 16
   disable_file_cache = false
   file_cache_max_size_hint = 2GB
   ```

Parameter	Description
disable_blob_cache	Specifies whether to cache data entry IDs. Valid values: ◦ *true*: Data entry IDs are not cached. ◦ *false*: Data entry IDs are cached.
max_blob_cache_weight	The maximum system memory that can be used by the cache for data entry IDs. Default value: 0.15. The value indicates 15% of the total system memory. The value must be between 0 and 1.
cache_prefix	The path in which the cached data entry IDs are stored. The value must be an absolute path.
max_retain_count	The maximum number of cached data entry IDs.
disable_file_cache	Specifies whether to cache metadata. Valid values: ◦ *true*: Metadata is not cached. ◦ *false*: Metadata is cached.
file_cache_max_size_hint	The maximum size of a metadata cache file. The actual size may exceed the specified value. Default value: 2 GB. Note ◦ If you set the parameter to 2 GB, you can back up a minimum of 4 TB of metadata. ◦ If you set the parameter to a small value, the backup does not fail but the cache performance is degraded. ◦ The value of the parameter cannot exceed the available disk space.

Notice

- The parameter settings take effect immediately after you save the hbr.config file. You do not need to restart the server or VM.
- The parameter settings are applied only to subsequent backup jobs. You cannot accelerate existing backup jobs by caching data entry IDs and metadata.

4.Configure a proxy server for the host of a backup client

This topic describes how to configure a Windows server as a proxy server for the host of a backup client.

Prerequisites

A proxy server is built.

If you encounter any problems when building a proxy server, see Step 1: Prepare a proxy server. This step describes the method to build the Apache HTTP server as a proxy server in Windows. The Apache HTTP server is a third-party service that is not provided by Hybrid Backup Recovery (HBR). The method is for reference only.

Context

If the host from which you want to back up data cannot access the Internet, you can configure a proxy server for the host.

Step 1: Prepare a proxy server

1. Prepare a server that has the Internet access.
2. Install Microsoft Visual C++ Redistributable for Visual Studio 2015-2019.

   VC_redist.x64.exe

   VC_redist.x86.exe
3. Download and decompress the package of Apache HTTP Server 2.4.
4. Modify the configuration file named *Apache24\conf\httpd.conf*.

   > **Note** Change the path in *Define SRVROOT "\Apache24"* to the installation directory of Apache. For example, if Apache is installed in the root directory of the D drive, you can change the path to *D:\Apache24*.

   - Load modules.

     ```
     LoadModule proxy_module modules/mod_proxy.so
     LoadModule proxy_connect_module modules/mod_proxy_connect.so
     LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
     LoadModule proxy_http_module modules/mod_proxy_http.so
     ```

   - Specify the listening port, for example, `Listen 8888`.
   - Set access permissions.

     ```
     ProxyRequests On
     ProxyVia On
     <Proxy *>
     Require all granted
     </Proxy>
     ```

5. Double-click `Apache24\bin\httpd.exe` to start the proxy service.

Step 2: Create a backup client

1. Log on to the HBR console.

   If the host runs a Linux operating system without a graphical user interface (GUI), use an intermediate host with a GUI as an agent to log on to the HBR console.

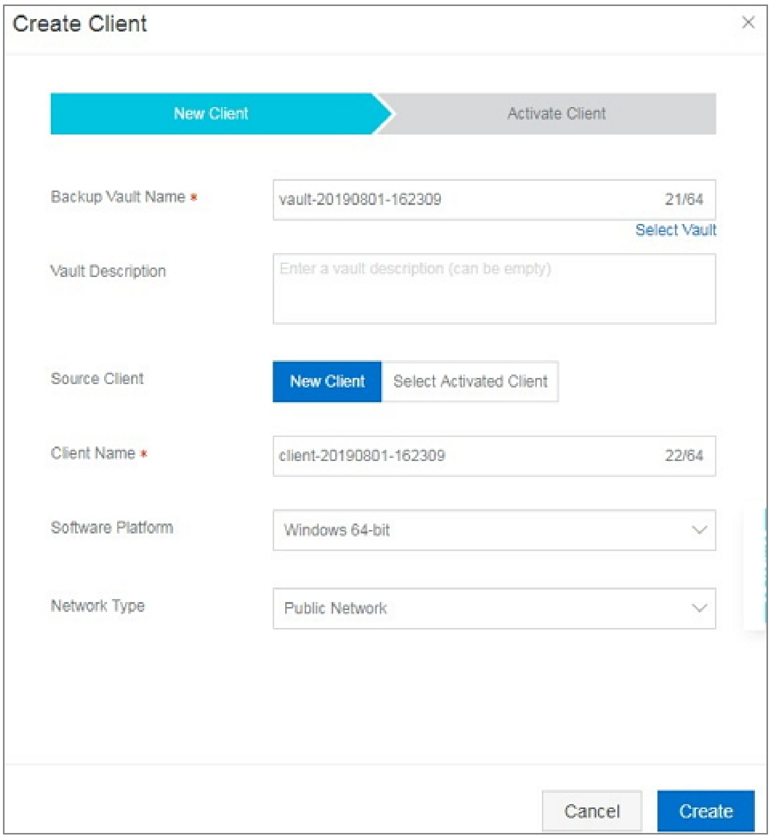
2. In the left-side navigation pane, choose **Backup > On-Premises Backup > File**.

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.



Create Client

Backup Vault Name *: vault-20190801-162309 21/64

Vault Description: Enter a vault description (can be empty)

Source Client: New Client

Client Name *: client-20190801-162309 22/64

Software Platform: Windows 64-bit

Network Type: Public Network

Parameter	Description

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 bytes 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 bytes in length.
Software Platform	The operating system that is running on the host from which you want to back up data. Valid values: ○ Windows 32-bit ○ Windows 64-bit ○ Linux 32-bit ○ Linux 64-bit
Network Type	○ **Virtual Private Cloud (VPC)**: Select this option if the host from which you want to back up data resides in a VPC and the VPC is in the same region as the backup vault. ○ **Public Network**: 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 backup or restore job.

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

> **Note** The backup client is used to connect the host to HBR. You can also download the backup client from the client list.

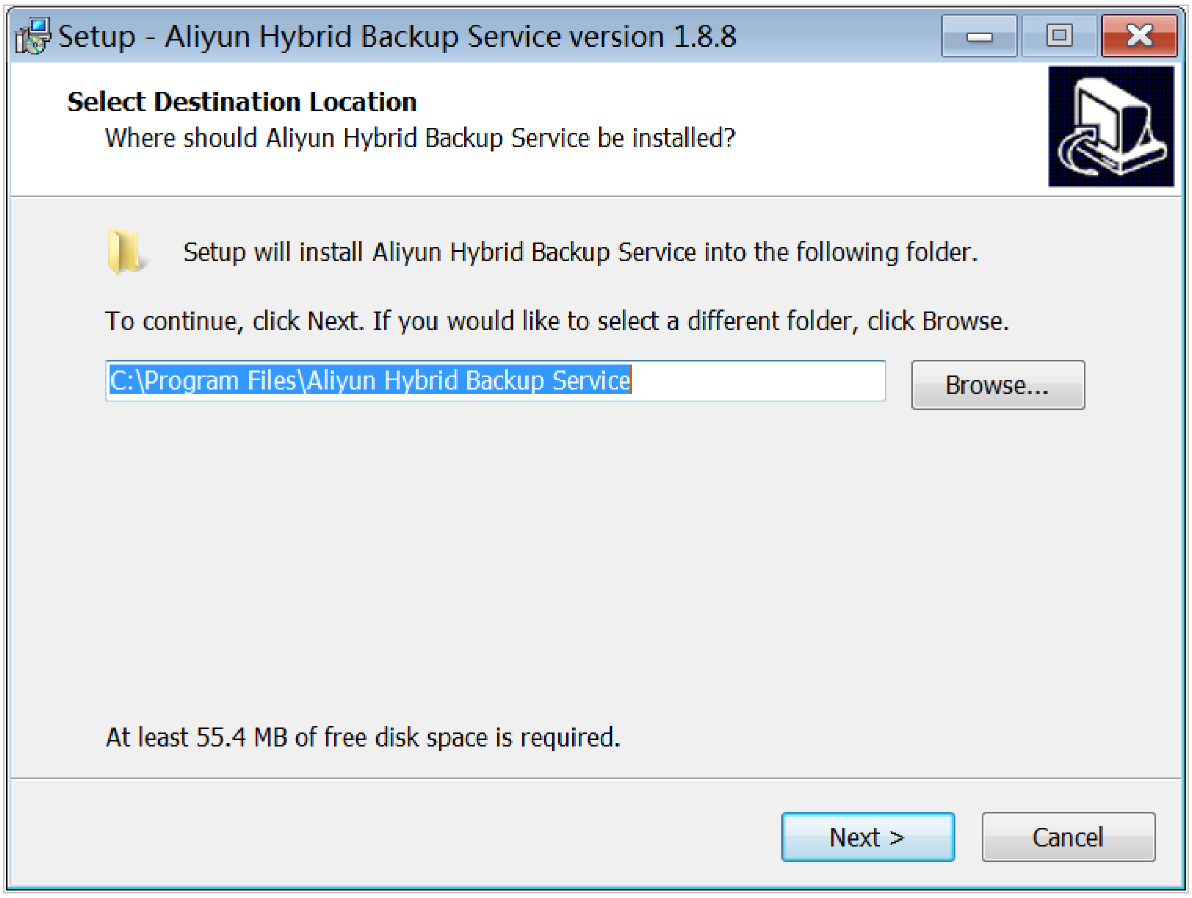
7. Click **Download Certificate**.

Step 3: Install the backup client

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 operational logs and an executable file are all stored in the installation directory.

- If the host 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 backup client.



Setup - Aliyun Hybrid Backup Service version 1.8.8

Select Destination Location

Where should Aliyun Hybrid Backup Service be installed?

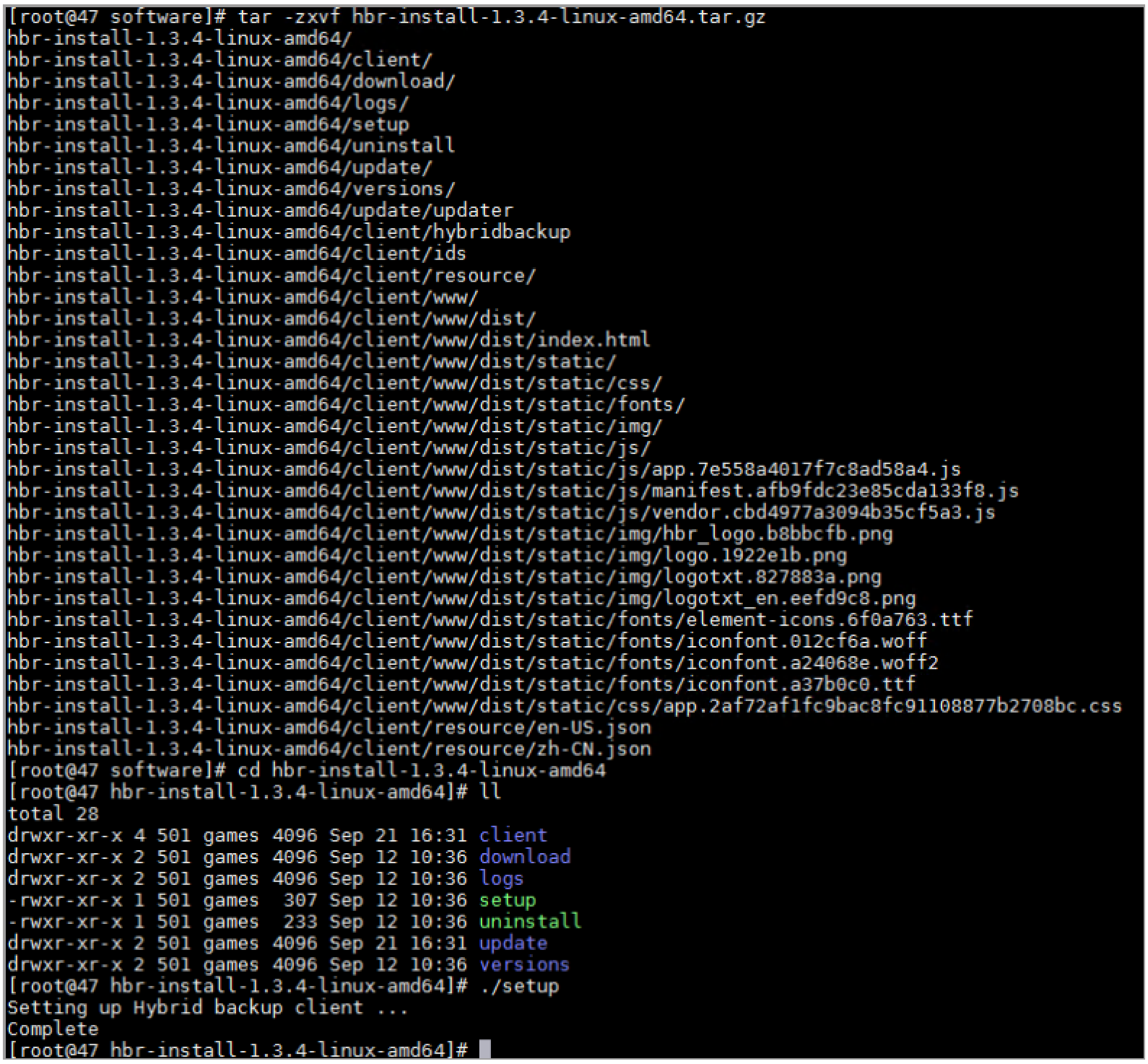
Setup will install Aliyun Hybrid Backup Service into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\Aliyun Hybrid Backup Service

At least 55.4 MB of free disk space is required.

- If the host runs Linux, decompress the installation package to a specified directory and run the `./setup` command to install the backup 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]# 
```

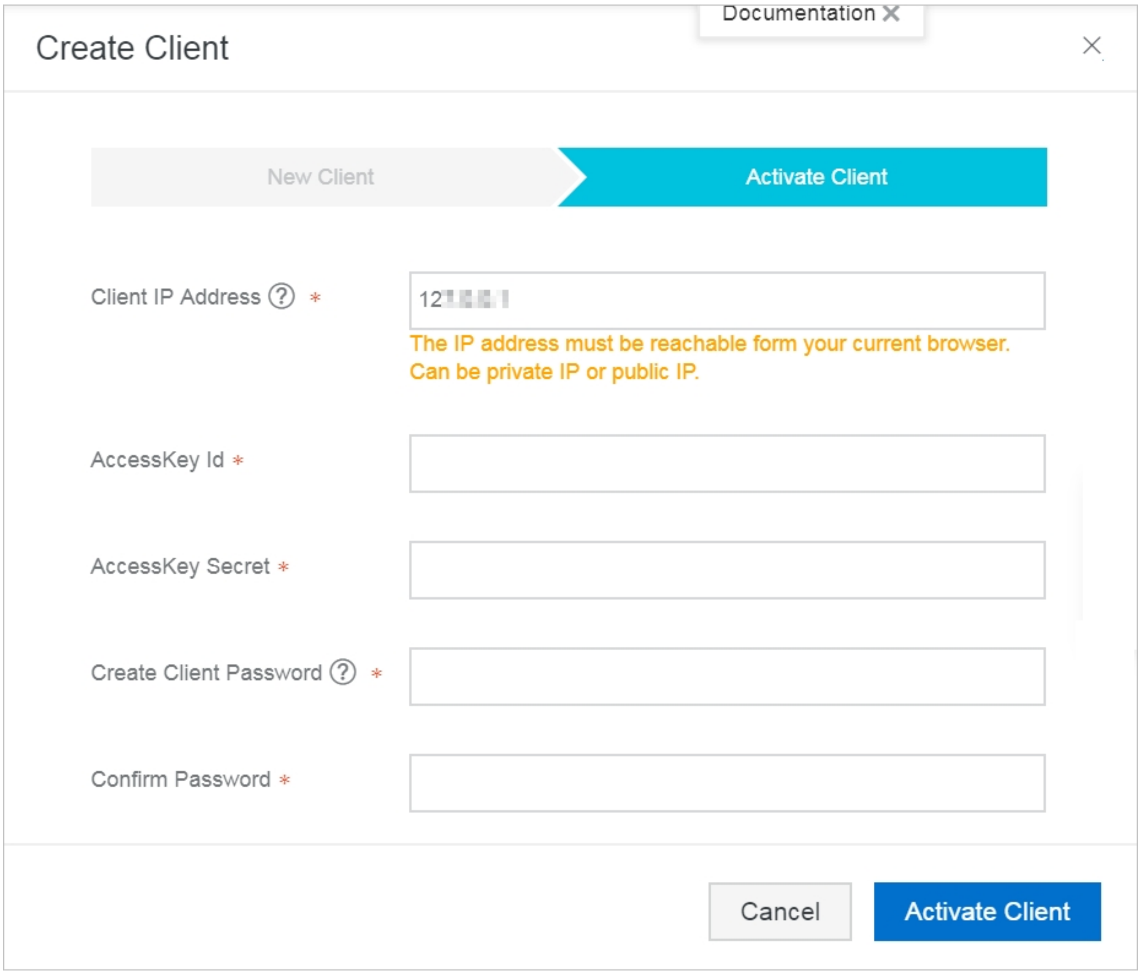
Step 4: Activate the backup client

After the backup client is installed, you can use the following methods to activate the backup client.

- Recommended. Activate the backup client in the HBR console.

  i. Log on to the HBR console.

  ii. 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 of the Add Client pane, set the following parameters.



Client IP Address ⓘ * 12[redacted]

The IP address must be reachable form your current browser. Can be private IP or public IP.

AccessKey Id *

AccessKey Secret *

Create Client Password ⓘ *

Confirm Password *

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. Specify the information if a proxy server is used for data transmission. **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 Channel Network Type	No	The type of the network that is used to send messages from HBR to the backup client.

iii. Click **Activate Client**.

The page of the backup client for files appears. You can then use the backup client to back up data. 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?

- Activate the backup client on the host

i. Enter the URL of the backup client in a browser to log on to the backup client. The URL is in the format of http://<Client IP address>:<Port number>, for example, *http://10****:8011*.

ii. On the **Register** page that appears, set the following parameters and click **Register**.

Parameter	Required	Description
Certificate File	Yes	The certificate of the backup client. Upload the certificate that you downloaded in Step 2: Create a backup client.
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	
Backup Data Network	No	The type of the network over which backup data is transferred. You can select **Public Network** or **Alibaba Intranet**.
Control Network Proxy	No	The information of the proxy server that is used to call the HBR API. The information includes the username, password, IP address, and listening port number of the proxy server. If identity authentication is not required, leave the username and password unspecified.

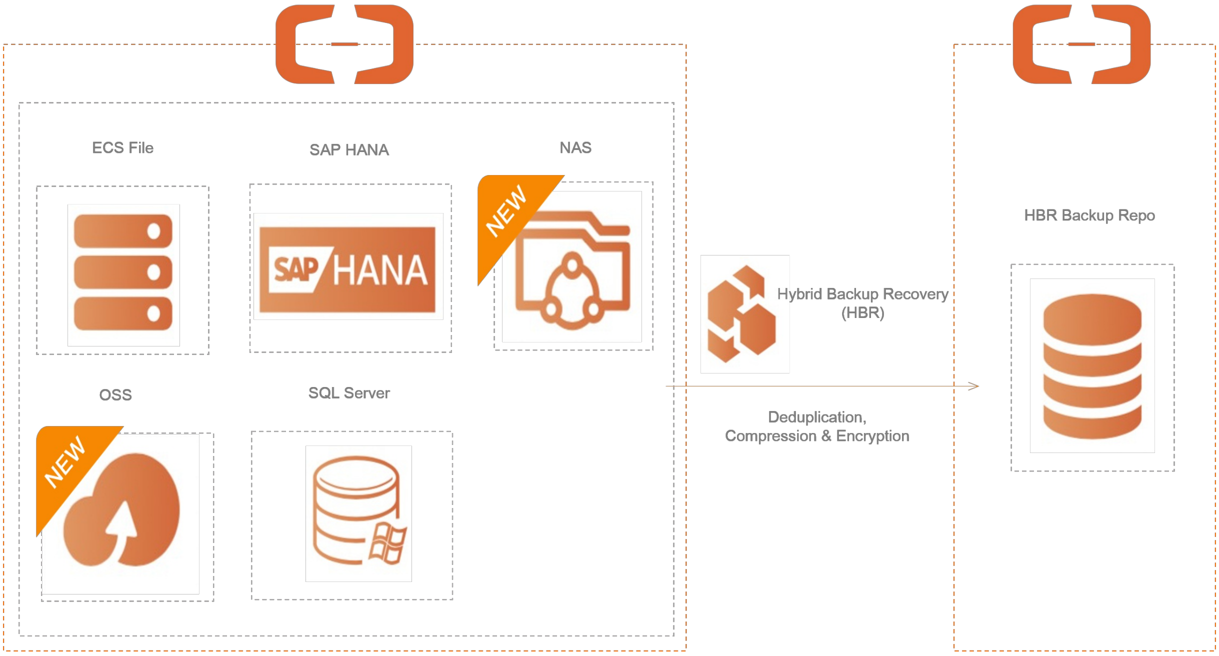
Parameter	Required	Description
Data Network Proxy	No	The information of the proxy server that is used to transmit backup data. Specify the information if a proxy server is used for data transmission. The information includes the username, password, IP address, and listening port number of the proxy server. If identity authentication is not required, leave the username and password unspecified.
Control Network Type	No	The type of the network that is used to call the HBR API.
Message Channel Network Type	Yes	The type of the network that is used to send messages from HBR to the backup client.

After the backup client for files is activated, you can use it to back up files.

5.Back up data from cloud resources

This topic describes the backup feature for cloud resources. You can use Hybrid Backup Recovery (HBR) to back up data from Alibaba Cloud resources and self-managed data centers in a secure and efficient way. This feature is suitable for Alibaba Cloud resources that are deployed on Elastic Compute Service (ECS), Apsara File Storage NAS, and Object Storage Service (OSS).

The following figure shows the architecture of the HBR backup feature. This feature is applicable to ECS file systems, NAS files, OSS files, self-managed SQL Server databases on ECS instances, and self-managed SAP HANA database resources on ECS instances. For more information, see Best practices for HBR-based backup of Alibaba Cloud resources.


ECS File
SAP HANA
NAS
NEW
OSS
NEW
SQL Server
Hybrid Backup Recovery (HBR)
Deduplication, Compression & Encryption
HBR Backup Repo

6.Enable the security enhancement feature for backup management

You can enable the security enhancement feature of Hybrid Backup and Recovery (HBR) to improve the security management of your data backup. This feature can protect your data against unexpected operations, malicious attacks, and unauthorized backup or restoration and help meet the requirements for data security and compliance. HBR allows you to encrypt your data based on Key Management Service (KMS), enable the immutable backup feature, and isolate backup permissions and recovery permissions. This topic describes how to enable the security enhancement feature for data backup.

Context

HBR provides the following features to support the security enhancement feature for data backup.

- KMS-based encryption

  KMS-based encryption allows you to manage your encryption key. You can encrypt the data in the backup source by using KMS before you store the backup data to the backup vault.

  > Notice
  >
  > - If you enable KMS-based encryption, you cannot modify a KMS key.
  > - If you disable or delete a KMS key, you cannot restore the backup data from the backup vault.
  > - We recommend that you configure the ID of a KMS key before you use the key to encrypt the data in the backup source. For more information, see Create a CMK.

- Immutable backup

  The immutable backup feature supports the Write Once Read Many (WORM) policy. If you enable this feature, you can write data to all backup vaults only once and read data from the backup vaults multiple times. The immutable backup feature provides additional protection for your backup vault.

  > Notice
  >
  > - If you enable the immutable backup feature, you cannot disable this feature.
  > - If you enable the immutable backup feature, you cannot delete the backup vault or backup data until the retention period expires.
  > - Backup and recovery operations are not affected.

- Isolation of backup permissions and recovery permissions

  You can grant backup or recovery permissions to a specified RAM user. This way, the RAM user can perform only backup or recovery operations but cannot perform both operations. This helps prevent unauthorized operations.

Enable KMS-based encryption

1. Prepare a KMS key.

   Before you use a KMS key to encrypt the data in the backup source, you must configure the ID of the KMS key. For more information, see Create a CMK.

2. On the Create Backup Plan page, set the **Source Encryption Type** parameter to *KMS* and specify the **KMS KeyId** parameter to create a backup plan. Then, you can enable the KMS-based encryption feature.
   On the **Storage Vaults** page, you can find **Encryption based on KMS** in the **Backup Type** column.

Enable immutable backup

1.
2. In the left-side navigation pane, choose **Backup Appliance > Storage Vaults**.
3. Find the backup vault for which you want to enable the immutable backup feature. In the **Actions** column to the right of the backup vault, choose **More > Modify Backup Vault**.
4. In the **Modify Backup Vault** panel, turn on **Immutable Backup**.
5. In the dialog box that appears, click **OK**.
6. In the **Modify Backup Vault** panel, click **OK**.
   After you click OK, **Yes** is displayed in the **Immutable Backup** column.

Isolate backup permissions and recovery permissions

1. Obtain the RAM policy that you can use to deny the backup permissions or recovery permissions for a backup vault.
   i.
   ii. In the left-side navigation pane, choose **Backup Appliance > Storage Vaults**.
   iii. Find the backup vault. In the **Actions** column to the right of the backup vault, choose **More > Modify Backup Vault**.
   iv. In the **RAM Permission Policy** section of the **Modify Backup Vault** panel, select the RAM policy that you can use to deny the backup permissions or recovery permissions.

- **RAM Policy that deny restore**

  Click the Copy button in the upper-left corner of the input box to copy the script. Example:

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "hbr:CreateRestore",
                "hbr:CreateRestoreJob",
                "hbr:CreateHanaRestore",
                "hbr:CreateUniRestorePlan",
                "hbr:CreateSqlServerRestore"
            ],
            "Resource": [
                "acs:hbr:*:1178037424989531:vault/v-0000ryfi******piu",
                "acs:hbr:*:1178037424989531:vault/v-0000ryfi******piu/client/*"
            ]
        }
    ]
}
```

> **Note** _v-0000ryfi******piu_ is the ID of the backup vault.

- **RAM Policy that deny backup**

  Click the Copy button in the upper-left corner of the input box to copy the script. Example:

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "hbr:CreateUniBackupPlan",
                "hbr:UpdateUniBackupPlan",
                "hbr:DeleteUniBackupPlan",
                "hbr:CreateHanaInstance",
                "hbr:UpdateHanaInstance",
                "hbr:DeleteHanaInstance",
                "hbr:CreateHanaBackupPlan",
                "hbr:UpdateHanaBackupPlan",
                "hbr:DeleteHanaBackupPlan",
                "hbr:CreateClient",
                "hbr:CreateClients",
                "hbr:UpdateClient",
                "hbr:UpdateClientSettings",
                "hbr:UpdateClientAlertConfig",
                "hbr:DeleteClient",
                "hbr:DeleteClients",
                "hbr:CreateJob",
                "hbr:UpdateJob",
                "hbr:CreateBackupPlan",
                "hbr:UpdateBackupPlan",
                "hbr:ExecuteBackupPlan",
                "hbr:DeleteBackupPlan",
                "hbr:CreateBackupJob",
                "hbr:CreatePlan",
                "hbr:UpdatePlan",
                "hbr:CreateTrialBackupPlan",
                "hbr:ConvertToPostPaidInstance",
                "hbr:KeepAfterTrialExpiration"
            ],
            "Resource": [
                "acs:hbr:*:1178037424989531:vault/v-0000ryfi******piu",
                "acs:hbr:*:1178037424989531:vault/v-0000ryfi******piu/client/*"
            ]
        }
    ]
}
```

> **Note** _v-0000ryfi******piu_ is the ID of the backup vault.

2. Log on to the RAM console and create a custom policy.

   For more information, see Create a custom policy.

3. Select the RAM user whose backup and recovery permissions you want to isolate. Then, attach the

policy that you created in to the RAM user.