ALIBABA CLOUD

Alibaba Cloud

Hybrid Backup

Back up ECS

Document Version: 20220407

Alibaba Cloud

Legal disclaimer

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

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

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

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

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

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

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

Document conventions

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

Table of Contents

1.Overview

is an easy-to-use data management service that is deployed in the public cloud to offer high agility, efficiency, security, and reliability. The service provides comprehensive protection that includes data backup and disaster recovery for Alibaba Cloud Elastic Compute Service (ECS) resources. The resources include ECS instances, databases on ECS instances, file systems on ECS instances, and ECS disks.

- ECS instance backup

  HBR is integrated with the Alibaba Cloud snapshot service to provide agentless backup for ECS instances. HBR ensures instance-level crash consistency and application consistency for ECS instances whose disks are of the ESSD type. HBR creates snapshots for each disk on an ECS instance to ensure data consistency for each disk of the non-ESSD type.

- ECS database backup

  HBR helps back up MySQL, Oracle, and SQL Server databases that are deployed on ECS instances.

- ECS file system backup

  HBR helps back up all files on ECS instances. You can restore the files based on your business requirements.

- ECS disk backup

  HBR is integrated with the Alibaba Cloud snapshot service to provide agentless backup for ECS instances and disks. You can use HBR to create crash-consistent snapshots for all disks, including system disks and data disks. Then, you can use these snapshots to back up or restore an entire disk.

2.ECS Server Backup

2.1. Overview

ECS instance backup is a service provided by HBR to protect the data on ECS instances by using disk snapshots. HBR provides automatic backup policies for ECS instances and a GUI console. In the HBR console, you can configure backup or restoration parameters. You can also perform restore, clone, and disaster recovery operations. You can manage backup files by using ECS instances instead of disks. This way, you can protect data on ECS instances in an efficient manner.

Scenarios

- **Back up or restore ECS instances**:

  HBR allows you to use automatic backup policies and ECS instance backup to back up or restore ECS instances.

- **Quickly build testing or development environments**:

  HBR allows you to clone a new ECS instance from the restoration point of an ECS instance within a few minutes. You can use the new ECS instance as a testing or development environment.

- **Implement cross-zone or cross-region disaster recovery at low costs**

  The clone feature for ECS instance backup allows you to create ECS instances in different zones. After you enable remote replication for ECS instances, you can use create new ECS instances to resume your services by using one of the remote resotration points.

Principles

ECS instance backup allows you to perform data backup and disaster recovery for ECS instances by using snapshots, snapshot-consistent groups, and remote snapshot replication.

1. After you configure a backup policy, HBR automatically creates snapshots for all disks based on the backup policy. A restoration point contains the snapshots that are created for all disks at a specific point in time.
2. If the type of all disks on an ECS instance is ESSD, HBR ensures the consistency of data on the ECS instance based on the snapshot-consistency group feature. If the type of disks on an ECS instance is ESSD, HBR creates snapshots for all disks at the same time. In this case, HBR cannot ensure the consistency of data between disks.
3. If you enable remote replication when you configure a backup policy, the snapshots in a restoration point are automatically replicated to a specified backup region. This way, you can back up data in a remote location.
4. When you restore an ECS instance, HBR uses the specified snapshots to roll back all disks to a specific point in time.
5. When you clone ECS instances or perform geo-disaster recovery, HBR creates disks from the snapshots of a specified restoration point, and then creates ECS instances based on the disks.

Billing

You are charged when you create ECS snapshots. ECS instance backup is a backup orchestration service that is provided by HBR based on the ECS snapshot capability. You are charged USD 0.005088 for each client per day when you use HBR clients to back up ECS instances. The fees are included into your HBR bills. Bills are generated on a daily basis. The fees for the storage usage of ECS snapshots that are used by this feature are included into the snapshot service bill. If you enable the remote replication feature, the fees for the storage usage of ECS snapshots that are replicated to the destination region and the fees for cross-region traffic are also included into the snapshot service bill. For more information, see Snapshots.

2.2. Create an ECS instance backup

is integrated with the Alibaba Cloud snapshot service to provide agentless backup for Elastic Compute Service (ECS) instances and disks. HBR can create crash-consistent snapshots for all disks, including system disks and data disks. You can use the snapshots to back up or restore an entire disk.

Prerequisites

To ensure crash consistency at the instance level, make sure that only enhanced SSDs (ESSDs) are attached to your instance. Otherwise, HBR enables the crash consistency feature only for single disks.

Context

- The ECS instance protection feature allows you to protect an ECS instance or specified disks by using a periodic disk backup strategy. This ensures long-term and low-cost protection.
- You are charged for the usage of ECS snapshots. ECS instance backup is a backup orchestration service that is provided by HBR based on the ECS snapshot capability. You are charged USD 0.005088 for each client per day when you use HBR to back up ECS instances. The fees are included into your HBR bills. Bills are generated on a daily basis. The fees for the storage usage of ECS snapshots that are used by this feature are included into the snapshot service bill. If you enable the remote replication feature, the fees for the storage usage of ECS snapshots that are replicated to the destination region and the fees for cross-region traffic are also included into the snapshot service bill. For more information, see Snapshots.

Precautions

You cannot use the ECS instance backup feature to back up or restore local disks. For more information, see Local disks.

If you use local disks to store data, your data may be lost. We recommend that you use the ECS file backup feature to protect your files in local disks and use the database backup feature to protect your databases deployed in local disks. For more information, see Back up files from ECS instances and Database backup.

Procedure

1.
2. In the left-side navigation pane, choose **Backup > ECS Server Backup**.
3.
4. In the upper-right corner of the page, click **+Add ECS Instance**.
5. In the **Create ECS Protection Plan** dialog box, configure the following settings:

i. Select the ECS instance that you want to protect.

> **Note** If you want to protect all disks of the ECS instance, turn on **Protect All Disks**. If you turn on Protect All Disks, all disks that are newly attached to the ECS instance are protected. If you want to protect only specific disks, turn off **Protect All Disks**.

ii. Configure a backup plan. The following table describes the parameters of a backup plan.

You can create backup files for an ECS instance at regular intervals based on a specified backup policy. You can also create only one backup file for the ECS instance at the current point in time.

Parameter	Description
On Schedule	If you turn on **On Schedule**, HBR creates backup jobs at regular intervals based on the specified backup policy.
Plan Name	This parameter is required only if you turn on **On Schedule**. The name of the backup plan. If you do not configure this parameter, a random name is specified for the backup plan.
Start Time	This parameter is required only if you turn on **On Schedule**. The start time of the scheduled backup plan. The time is accurate to seconds.
Backup Interval	This parameter is required only if you turn on **On Schedule**. The interval at which HBR runs backup jobs. Unit: hours, days, or weeks.
Retention Period	The period of time for which HBR retains backup files. Unit: days, weeks, months, or years.

iii. (Optional)Click **Application Consistent Backup**.

This feature is available only in the Singapore (Singapore) and China (Hong Kong) regions. For more information, see Enable the application-consistent backup feature.

iv. (Optional)Turn on **Cross-Region Copy** to enable the cross-region replication feature and then configure the parameters. The following table describes the parameters.

Parameter	Description
Destination Region	If you enable the cross-region replication feature, the backup files that are created by the backup plan are automatically replicated to a specified destination region. If a source ECS instance is infected with viruses or you accidentally deleted data, you can use backup files in the source region or backup files that are replicated to the destination region to create an ECS instance to restore data.
Retention Period	The retention period for the backup data in the destination region. Unit: days, weeks, months, or years.

6. Click **OK**.

   After you create the backup policy, HBR runs the first backup job at the start time that you specify and runs the subsequent backup jobs based on the interval that you specify.

What to do next

The following table describes the tabs that are provided by the ECS instance backup feature. You can use the tabs to efficiently manage backup jobs.

Tab	Description	Operations
Protected ECS Instances	Shows the protected ECS instances.	• **Protect Now**: Specify all or some disks for protection. You can configure the Retention Period and Long-term Backup parameters. • **Stop Protection**: Stop protection for an ECS instance. **Notice** If you stop protection for an ECS instance, the ECS instance is removed from the protected ECS instance list and all protection plans of the ECS instance are deleted. The generated ECS instance backups are retained. If you want to delete a backup file of an ECS instance, click the backup point of the backup file in the backup history and then click Delete. • **Resume Plan**: You can resume a suspended protection plan. • **Suspend Plan**: If you suspend a protection plan, no backup protection is performed. • **Delete Plan**: If a protection plan expires, you can delete the protection plan. • **Modify**: If an existing protection plan no longer meets your requirements, you can modify the protection plan.

Tab	Description	Operations
Protection Plans	Shows the protection plans that you configured. On the tab, you can perform basic O&M operations on the protection plans.	• **Run Now**: Immediately execute a protection plan. • **Modify**: Modify a protection plan. • **Suspend Plan**: If you suspend a protection plan, no backup protection is performed. • **Delete Plan**: If a protection plan expires, you can delete the protection plan. • **Batch Immediate Execution**: Immediately execute multiple protection plans at the same time. • **Batch Update Policy**: Update the backup policies and replication policies of multiple protection plans at the same time.
Jobs	Shows the status of executed jobs.	You can cancel the jobs that are being executed.
Batch Add ECS	Creates multiple backup files for an ECS instance. You can create up to 50 backup files for an ECS instance at a time.	In the upper-right corner of the ECS Server Backup page, click **Batch Add ECS**. Follow the instructions to select an ECS instance and configure a protection plan.

What's next

- Restore an ECS instance
- Restore a disk

2.3. Enable the application-consistent backup feature

provides the application-consistent backup feature based on Cloud Assistant and the backup service. The application-consistent backup feature helps prevent unexpected startup operations during data restore, for example, log restore operations at the startup of database applications. This way, all applications start in a consistent state.

Prerequisites

- A public IP address or an elastic IP address (EIP) is configured for your ECS instance. This way, the ECS instance allows access over the Internet.
- Your ECS instance runs one of the following operating systems:
  - Windows: Windows Server 2019, Windows Server 2016, and Windows Server 2012.
  - Linux: CentOS version 7.6 and later, Ubuntu version 18.04 and later, and Alibaba Cloud Linux version 2 (2.1903 LTS 64-bit).
- All disks that are attached to your ECS instance are enhanced SSDs (ESSDs) and the file systems are ext3, ext4, XFS, or New Technology File System (NTFS).

- Your ECS instance is created in the Singapore (Singapore) or China (Hong Kong) region.

Context

By default, creates crash-consistent backup files based on the Alibaba Cloud snapshot service. If you enable the application-consistent backup feature when you create a backup file for an ECS instance, HBR creates an application-consistent backup file based on the actual scenario.

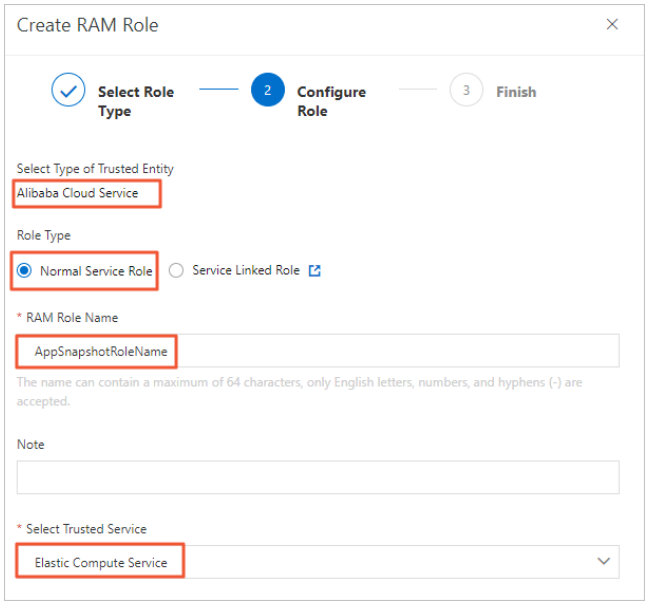
The application-consistent backup feature helps back up in-memory data and in-progress database transactions when backup files are being created. This way, the consistency between the application data and database transactions is ensured. The application-consistent backup feature helps prevent data corruption, data loss, and log restore operations at the startup of database applications. This way, all applications start in a consistent state.

Step 1: Configure a RAM role for the ECS instance

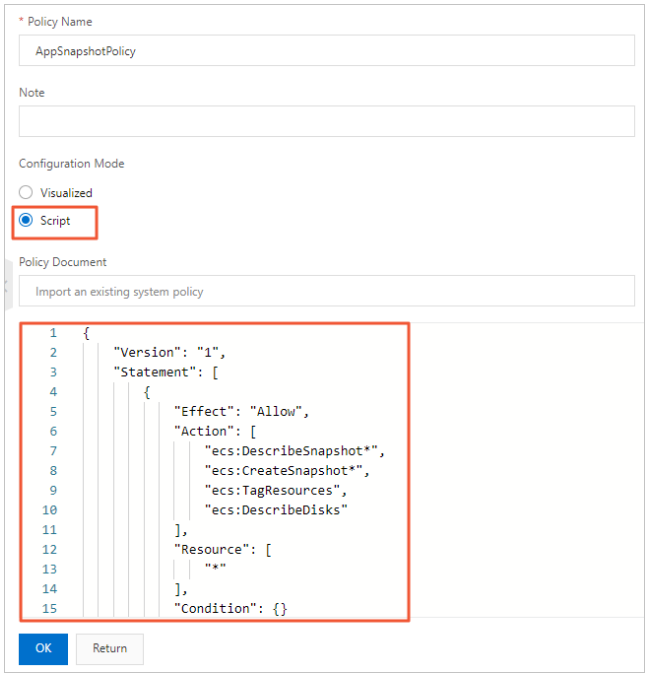
Before you enable the application-consistent backup feature, you must configure a RAM role for the ECS instance.

1. Log on to the RAM console by using your Alibaba Cloud account.
2. Create a RAM role for the application-consistent backup feature. For more information, see Create a RAM role for a trusted Alibaba Cloud service.

   The following figure shows how to create the AppSnapshotRoleName RAM role.



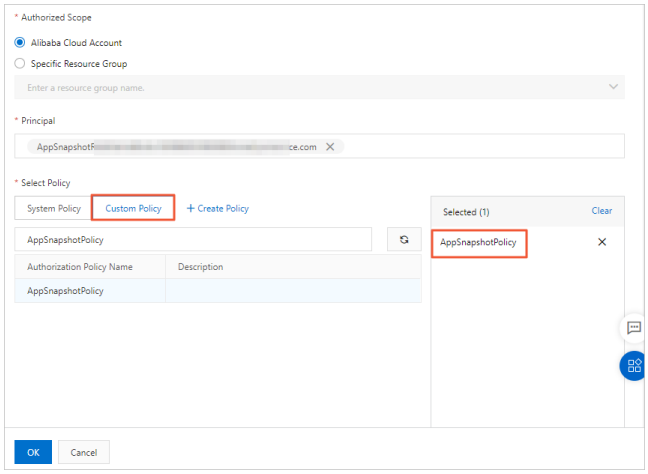
3. Create a policy for the application-consistent backup feature. For more information, see Create a custom policy.



Create the AppSnapshotPolicy policy, which grants the permissions to query snapshot details, create snapshots, configure tags, and query disk details. You can use the following policy:

```
{ "Version": "1", "Statement": [ { "Effect": "Allow", "Action": [ "ecs:DescribeSnapshot*", "ecs:CreateSnapshot*", "ecs:TagResources", "ecs:DescribeDisks" ], "Resource": [ "*" ], "Condition": {} } ] }
```

4. Attach the AppSnapshotPolicy policy to the AppSnapshotRoleName RAM role. For more information, see Grant permissions to a RAM role.



5. Attach the AppSnapshotRoleName RAM role to the ECS instance. For more information, see Attach an instance RAM role.

Step 2: Enable the application-consistent backup feature

For Windows ECS instances, you can use Volume Shadow Copy Service (VSS) to implement application consistency.

For Linux ECS instances, you must configure shell scripts (pre-freeze and post-thaw scripts) based on the applications deployed on the instances to implement application consistency.

1.
2. In the left-side navigation pane, choose **Backup > ECS Server Backup**.
3.
4. In the upper-right corner of the page, click **+Add ECS Instance**.
5. In the **Create ECS Protection Plan** dialog box, configure the following settings:
   i. Select the ECS instance that you want to protect.

   > **Note** If you want to protect all disks of the ECS instance, turn on **Protect All Disks**. If you turn on Protect All Disks, all disks that are newly attached to the ECS instance are protected. If you want to protect only specific disks, turn off **Protect All Disks**.

   ii. Configure a backup plan. The following table describes the parameters of a backup plan.

   You can create backup files for an ECS instance at regular intervals based on a specified backup policy. You can also create only one backup file for the ECS instance at the current point in time.

Parameter	Description
On Schedule	If you turn on **On Schedule**, HBR creates backup jobs at regular intervals based on the specified backup policy.
Plan Name	This parameter is required only if you turn on **On Schedule**. The name of the backup plan. If you do not configure this parameter, a random name is specified for the backup plan.
Start Time	This parameter is required only if you turn on **On Schedule**. The start time of the scheduled backup plan. The time is accurate to seconds.
Backup Interval	This parameter is required only if you turn on **On Schedule**. The interval at which HBR runs backup jobs. Unit: hours, days, or weeks.
Retention Period	The period of time for which HBR retains backup files. Unit: days, weeks, months, or years.

   iii. Select **Application Consistent Backup**.

   - Enable the application-consistent backup feature for a Windows ECS instance

   > **Note** If you select **Application Consistent Backup**, you must install a Cloud Assistant client on the ECS instance. In Windows, the process of a Cloud Assistant client is named `AliyunService`. For more information, see Overview.

- Enable the application-consistent backup feature for a Linux ECS instance

  Write the application pre-freeze and post-thaw scripts based on the applications deployed on the ECS instance and upload the scripts to the ECS instance.

  You can use the FTP service or Cloud Assistant to upload the application pre-freeze and post-thaw scripts to the ECS instance.

  - **Application pre-freeze scripts**: Run the `chmod 700 /tmp/prescript.sh` command to grant the read, write, and execute permissions on the scripts only to the root user. /tmp/prescript.sh is the save path of the scripts.
  - **Application post-thaw scripts**: Run the `chmod 700 /tmp/postscript.sh` command to grant the read, write, and execute permissions on the scripts only to the root user. /tmp/postscript.sh is the save path of the scripts.

  > **Notice**
  > - If **Application Consistent Backup** is selected and the scripts are configured as expected, HBR creates application-consistent backup files.
  > - If **Application Consistent Backup** is selected but no scripts are configured or the scripts are not configured as expected, HBR creates file system-consistent backup files.

  Sample scripts for the application-consistent feature:

  - Download the application-consistent scripts for MySQL.

    After you download and deploy the scripts, you must specify the password of a MySQL database in the scripts.

  - Download the application-consistent scripts for Oracle.

    After you download and deploy the scripts, you must specify the installation path of an Oracle database in the scripts.

  > **Note** If you select **Application Consistent Backup**, you must install a Cloud Assistant client on the ECS instance. In Linux, the process of a Cloud Assistant client is named `aliyun.service`. You can run the `ps aux|grep aliyun.service` command to check whether a Cloud Assistant client is installed. For more information, see Overview.

iv. Click **OK**.

2.4. Restore an ECS instance

A system failure occurs or an unexpected operation is performed on an Elastic Compute Service (ECS) instance. You can use the clone or restore feature of a backup file to restore the ECS instance to a specified point in time. This topic describes how to restore an ECS instance.

Prerequisites

A backup file is created for the ECS instance. For more information, see Create an ECS instance backup.

Use the clone feature to restore an ECS instance

A system failure occurs or an error operation is performed on an ECS instance. In this case, you can use the clone feature of a backup file to restore the ECS instance to a specified point in time.

1.
2. In the left-side navigation pane, choose **Backup > ECS Server Backup**.
3.
4. Click the **Protected ECS Instances** tab.
5. Click the icon next to the ECS instance.
6. On the **Instance Protection** tab, click a backup file and then click **Clone**.
7. In the **Create ECS Instance from Backup** panel, enter a hostname and an instance name, and then select a VPC and a vSwitch.
8. Click **Create**.

> **Note** You are charged for the new ECS instance based on the billing rules of ECS. For more information, see ECS pricing.

After you create the ECS instance, you can view the cloning progress on the **Jobs** tab.

Directly restore an ECS instance

A system failure occurs or an unexpected operation is performed on an ECS instance. In this case, you can use a backup file to restore the ECS instance to a specified point in time.

1.
2. In the left-side navigation pane, choose **Backup > ECS Server Backup**.
3.
4. Click the **Protected ECS Instances** tab.
5. Click the icon next to the ECS instance.
6. On the **Instance Protection** tab, click a backup file and click **Restore**.

> **Notice** You can restore an ECS instance only if the ECS instance is stopped and no backup file is being created for the ECS instance. After a disk is restored to a specified point in time, the data that is written to the disk after the point in time is cleared. Proceed with caution.

7. In the message that appears, click **OK**.
   After you create the restore job, you can view the progress on the **Jobs** tab.

2.5. Restore a disk

A system failure occurs or an unexpected operation is performed on a disk that is attached to an Elastic Compute Service (ECS) instance. In this case, you can use a backup file for the disk in the source region or a backup file that is replicated to the destination region to restore data or create a new disk to restore data.

Prerequisites

A backup file is created for the ECS instance For more information, see Create an ECS instance backup.

Context

The disk backup feature can protect all disks that are attached to an ECS instance. The protection applies to disks that you want to attach in the future. You can also use this feature to protect specific disks. You can use a backup file to efficiently restore a disk based on your business requirements.

Restore a disk

1.
2. In the left-side navigation pane, choose **Backup > ECS Server Backup**.
3.
4. Click the **Protected ECS Instances** tab.
5. Click the icon next to the ECS instance.
6. On the **Disk Protection** tab, click a backup file and then click **Restore**.

   > **Notice** A disk can be restored only if the ECS instance is stopped and no backup file is being created for the disk. After a disk is restored to a specified point in time, the data that is written to the disk after the point in time is cleared. Proceed with caution.

7. In the message that appears, click **OK**.
   After you create the restore job, you can view the progress on the **Jobs** tab.

Create a disk

1.
2. In the left-side navigation pane, choose **Backup > ECS Server Backup**.
3.
4. Click the **Protected ECS Instances** tab.
5. Click the icon next to the ECS instance.
6. On the **Disk Protection** tab, click a backup file and then click **Clone**.
7. In the **Create Disk from Backup** panel, select the ECS instance to which you want to attach the new disk. Click **Next**.
8. In the **Set Mount Parameters** step, select a disk type and click **Create**.
   After you create the disk, you can view the restore progress on the **Jobs** tab.

3.Disk Backup

3.1. Create disk backups

is integrated with the Alibaba Cloud snapshot service to provide agentless backup for Elastic Compute Service (ECS) instances and disks. HBR can create crash-consistent snapshots for all disks, including system disks and data disks. You can use these snapshots to back up or restore an entire disk.

Context

Backup for ECS disks is a backup orchestration service that is provided by HBR based on the snapshot feature of ECS. You are billed for the usage of the Alibaba Cloud snapshot service. For more information, see Snapshots.

Precautions

You cannot use the disk backup feature to back up or restore local disks. For more information, see Local disks.

If you use local disks to store data, your data may be lost. We recommend that you use the ECS file backup feature to protect your files in local disks and use the database backup feature to protect your databases deployed in local disks. For more information, see Back up files from ECS instances and Database backup.

Procedure

Notice When you add an ECS instance and disks, make sure that the disks are in the **In Use** or **Unattached** state. If the disks are in the In Use state, the ECS instance must be in the **Running** or **Stopped** state.

1.
2. In the left-side navigation pane, choose **Backup > Disk Backup**.
3.
4. In the upper-right corner of the Disk Backup page, click **Disk Backup Wizard**.
5. In the **Disk Backup Wizard** panel, select the disk that you want to back up and click **Next**.
6. In the **Configure Backup Policy** step, set the Backup Type parameter to **Manual Backup** or **Auto Backup**.
   - **Manual Backup**

     If Manual Backup is specified, you must enter the name of the backup file in the **Backup Name** field.

     The name must be 2 to 128 characters in length, and can contain only the following special characters: periods (.), underscores (_), hyphens (-), and colons (:). The name cannot start with auto, a special character, or a digit.
   - **Auto Backup**

     If Auto Backup is specified, you can select a backup policy from the drop-down list. You can also click **Create Backup Policy** and set the parameters to create an automatic backup policy. The following table describes the parameters.

Parameter	Description
Policy Name	The name of the custom policy.
Backup Time	The time at which you want to run a backup job.
Backup Week	One or more days on which you want to run backup jobs in a week.
Retention Period	The period of time for which backup files are retained in the source region. ■ *Custom*: You can specify a retention period. Valid values: 1 to 65536. Unit: days. ■ *Always Keep*: Backup files in the source region are stored permanently.
Replication to Other Region	If you enable the cross-region replication feature, the backup files that are created by the backup plan are automatically replicated to a specified destination region. ■ Backup files can be replicated between the China (Hong Kong) and Singapore (Singapore) regions. ■ If the ECS instance is infected with viruses or data is lost due to accidental deletion, you can use backup files in the source region or backup files replicated to the destination region to create an instance or a disk to restore data. Valid values: ■ *Enabled* ■ *Not Enabled*
Destination Region	You must specify a value for this parameter only if the **Replication to Other Region** parameter is set to *Enabled*. The destination region to which you want to replicate the backup files.
Replicated Backup Point Retention Period	You must specify a value for this parameter only if the **Replication to Other Region** parameter is set to *Enabled*. The period of time for which you want to retain the backup files that are replicated to the destination region. ■ *Custom*: You can specify a retention period. Valid values: 1 to 65536. Unit: days. ■ *Always Keep*: Backup files in the destination region are stored permanently.

7. Click **OK**.
   After the backup policy is created, you can view the progress of the disk backup on the **Protected Disk** tab.

What's next

Restore a disk

3.2. Restore a disk

A system failure occurs or an unexpected operation is performed on a disk that is attached to an Elastic Compute Service (ECS) instance. In this case, you can use a backup file in the source region or a backup file replicated to the destination region to restore the original disk or create a new disk to restore data. This topic describes how to restore a disk.

Prerequisites

A backup file is created for a disk. For more information, see Create disk backups.

Context

The disk backup feature can protect all disks that are attached to ECS instances, including the disks that are subsequently attached. You can also use the feature to protect specified disks. To restore a disk, you can use a backup file in the source region or a backup file that is replicated to the destination region.

Restore a disk

If a system failure occurs or an error operation is performed on a disk that is attached to an ECS instance, you can use an existing backup file to restore the ECS disk.

1.
2. In the left-side navigation pane, choose **Backup > Disk Backup**.
3.
4. Click the **Protected Disk** tab.
5. Click the + icon next to the disk that you want to restore.
6. On the **Backups** tab, click a backup file in the source region or a backup file that is replicated to a destination region, and click **Restore**.

   > **Notice** A disk can be restored only if the ECS instance is stopped and no backup file is being created for the disk. After you restore an ECS disk to a point in time, the data that is written to the ECS disk after the point in time is cleared. Proceed with caution.

7. In the **Restore** panel, set the Enable Auto Startup parameter and click **Create**.

Create a disk

If a system failure occurs or an unexpected operation is performed on a disk that is attached to an ECS instance, you can use an existing backup file to restore the disk.

1.
2. In the left-side navigation pane, choose **Backup > Disk Backup**.
3.
4. Click the **Protected Disks** tab.
5. Click the + icon next to the disk that you want to restore.
6. On the **Backups** tab, click a backup file in the source region or a backup file that is replicated to a

destination region, and click **Clone**.

7. In the **Clone** panel, select a zone and disk type and click **Create**.

> **Notice** Backup files that are replicated to a destination region can be used only to restore data.

Replicate the backup file of a disk to a remote region

You can replicate the backup file of a specified disk to a destination region.

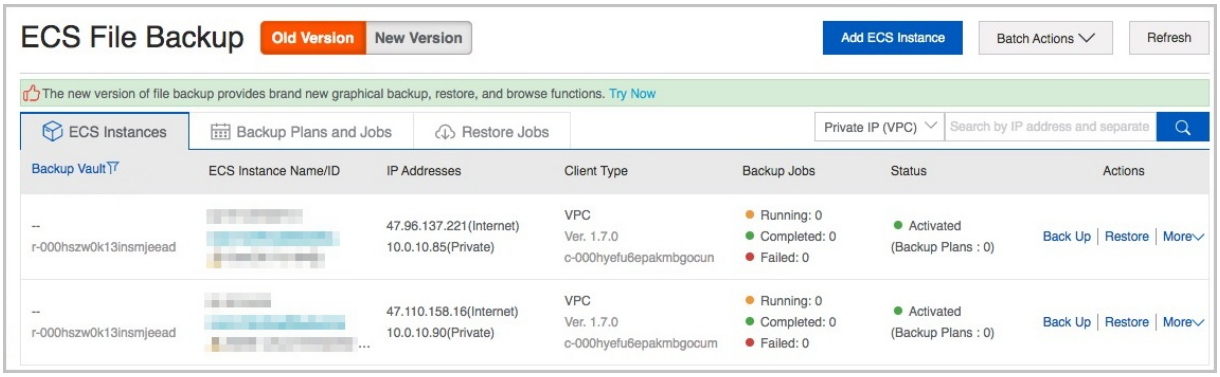
1.
2. In the left-side navigation pane, choose **Backup > Disk Backup**.
3.
4. Click the **Protected Disks** tab.
5. Click the icon next to the disk that you want to restore.
6. On the **Backups** tab, click a backup file in the source region or a backup file that is replicated to a destination region, and click **Copy**.
7. In the **Copy** panel, select a destination region, specify a name and description for the backup file, and then click **Create**.

4.Differences between two versions of the ECS file backup feature

This topic describes the differences between two versions of the ECS file backup feature.

Upgrade notes

You can use the latest version on a more comprehensive and user-friendly interface in the Hybrid Backup Recovery (HBR) console. We recommend that you upgrade your backup client with one click. We will offer technical support if you have questions. The earlier versions will become unavailable after January 1, 2021. You must upgrade all ECS backup clients of earlier versions before June 30, 2021. Click **Upgrade** in the Client Type column to upgrade the client.



> **Note**
>
> - The upgrade takes about 3 minutes.
> - After the upgrade is complete, the current backup instance is deleted from the ECS instance list on the **Old Version** tab, and appears in the ECS instance list on the **New Version** tab.

Version comparison

HBR provides the latest version of the ECS file backup feature based on the earlier versions. You can use the latest version to back up files on a more comprehensive and user-friendly interface in the HBR console. The following table describes the differences between the two versions of the ECS file backup feature.

Item	Earlier versions of ECS file backup	Latest version of ECS file backup
General backup restoration	Supported.	Supported.
Backup search	Not supported.	Supported.
Classic network support	Only the China (Beijing) region is supported.	Supported.
One-click ECS file backup	Not supported.	Supported.
Visualize recovery points	Not supported.	Supported.

Item	Earlier versions of ECS file backup	Latest version of ECS file backup
Preset plan templates.	Not supported.	Supported.
Job management	Backup plans can only be viewed.	Supported.

5.ECS file backup (new)

5.1. 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 for Elastic Compute Service (ECS) to back up files from an ECS instance in the HBR console. You can then restore the files if they are lost or damaged. HBR backs up and restores files in the streaming mode.

You can perform the following operations to back up files from and restore files to ECS instances:

- Prepare for data backup
- Back up files from ECS instances
- Restore files to an ECS instance

> **Note** For more information about how to back up on-premises files, see Overview.

5.2. Prepare for data backup

You can use Hybrid Backup Recovery (HBR) to back up files from Elastic Compute Service (ECS) instances and restore the files as needed. This topic describes how to prepare for data backup.

Usage notes

- To optimize the backup speed, we recommend that you run a backup client on an ECS instance that has the following configurations: 64-bit processors, two or more CPU cores, and more than 8 GB of available memory.
- The volume of data that can be backed up depends on the available memory. If a backup client has 4 GB of available memory, up to one million files or 8 TB of data can be backed up. If you want to back up tens of millions of files, we recommend that you configure 16 GB of available memory for the backup client.

Step 1: Create and assign the AliyunServiceRoleForHbrEcsBackup role

Before you use HBR to back up files from ECS, you must create the AliyunServiceRoleForHbrEcsBackup role and assign the role to HBR. To create and assign the role, perform the following steps:

1.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
   In the dialog box that appears, create and assign the role as prompted.
3. In the **Hybrid Cloud Backup Service Authorization** dialog box, click **Confirm Authorization**.

   For more information, see Service-linked roles.

Step 2: Install Cloud Assistant

An HBR backup client for ECS must be used together with Cloud Assistant.

- If the ECS instance that you need to back up was purchased before December 1, 2017, you must install the Cloud Assistant client. For more information, see Install the Cloud Assistant client.

- If the ECS instance that you need to back up was purchased on or after December 1, 2017, the Cloud Assistant client is pre-installed.

5.3. Back up files from ECS instances

This topic describes how to use Hybrid Backup Recovery (HBR) to back up ECS files.

Prerequisites

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

Create a backup plan

1.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
3. In the top navigation bar, select a region.
4. On the **ECS File Backup** page, click **New Version**.
5. On the **ECS Assets** tab, find the ECS instance for which you want to create a backup plan. Then, click **Back Up** in the **Actions** column.
6. In the **Create Backup Plan** panel, set the parameters and click **OK**.

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 where HBR stores backup data in the cloud. You can back up files from multiple HBR backup clients to a single vault. Backup vaults reside in different regions. You can select or create a backup vault only in the current region.
Vault Name	Select a backup vault where HBR stores backup data from the drop-down list.
Plan Name	The name of the backup plan. By default, a random name is used.

Parameter	Description
Backup Rules	Select **All Folders** or **Specified Folders**. ◦ If you select **All Folders**, you must select whether to turn on **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. To specify multiple source paths, click **Add Folders**. Specify the paths based on the following rules: ▪ If the source path does not contain an asterisk (*) wildcard, you can enter up to eight source paths. ▪ If the source path contains an asterisk (*) wildcard, 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 VSS backup is used, you can enter only one path. UNC paths or wildcards (*) are not supported. You cannot exclude files from the backup plan. ▪ If UNC paths are used, VSS paths or 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.
Exclude System Folders	If you turn on **Exclude System Folders**, system folders are not backed up.
Backup File Type	You can select **All Types** or **Specified Type**. If you select **All Types**, all types of files are backed up. If you select **Specified Type**, you must select the types of the files that you want to back up from the **Select File Type** drop-down list.
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.

Parameter	Description
Retention Policy	You can 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**, the backup files are permanently retained.
Retention Period	This parameter is required only if the Retention Policy parameter is set to **Limited**. The retention period of backup data. Units: days, weeks, months, and years.
Use VSS	This feature is available only for Windows. If you turn on **Use VSS**, the Volume Shadow Copy Service (VSS) is used during backup. Then, you can enter only one path. UNC paths or wildcards (*) are not supported. You cannot exclude files from the backup plan.
Throttle Bandwidth	Specifies whether to throttle the bandwidth. You can limit the bandwidth used for data backup during peak hours to guarantee business continuity. If you turn on Throttle Bandwidth, 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

On the **ECS Assets** tab, find the ECS instance that you want to back up. In the **Actions** column, perform the following operations:

- Use HTTPS to transmit data.

  If you use HTTPS to transmit data, the performance of data transmission is compromised. If you change the setting of this parameter, the change takes effect on the next backup or restoration 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 described in the following table.

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.

Alert policy	Description
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 restoration 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 restoration 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 to an ECS instance

5.4. Restore files to an ECS instance

You can restore files to an Elastic Compute Service (ECS) instance from a backup of the ECS instance, or from another ECS instance in the same backup vault. You can also restore files to an ECS instance from a backup of an on-premises client.

Prerequisites

Files are backed up from ECS instances. For more information, see Back up files from ECS instances.

Create a restoration job

1.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
3. In the top navigation bar of the page, select the region where the instance is deployed.
4. On the **ECS File Backup** page, click **New Version**.
5. On the **Backup Plans** tab, click the icon on the left of a completed backup plan.
6. Specify a point in time 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**.

You can set the following three parameters:

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 file 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 restoration 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 file 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 restoration 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`

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.
Client Name	The client to which files are restored.

iii. Specify the restoration 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 restoration job is created, you can view the job progress in the **Status** column on the **Restore Jobs** tab.

5.5. 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 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

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.

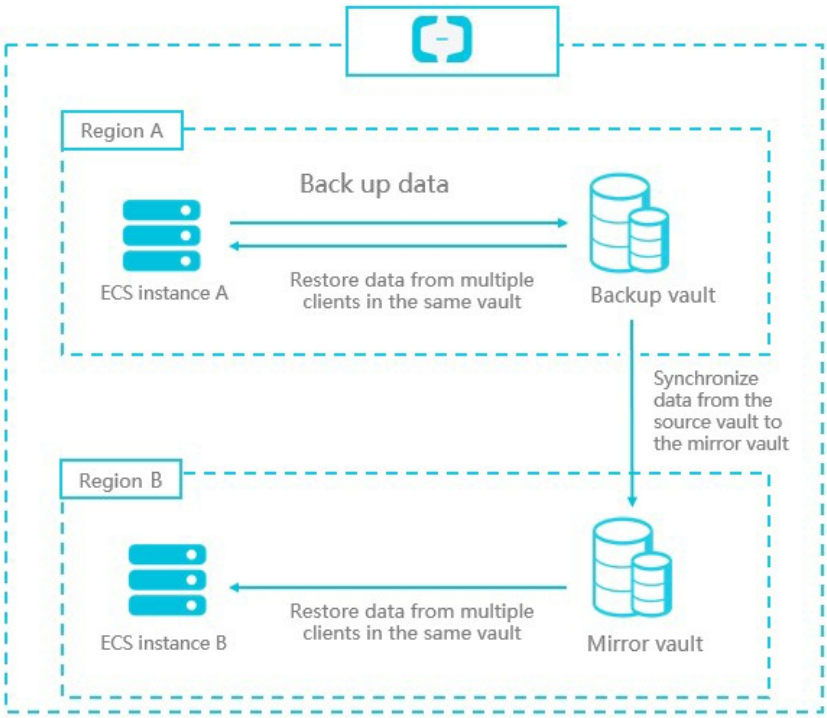
Alert policy	Description
Disabled	The backup client does not send alert notifications.
Same as Vault	If you select this option, the client uses the alert policy of the backup vault.
Default	The backup client sends alert notifications to the owner of the Alibaba Cloud account by using emails.
Custom	If 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**.

5.6. Restore files across regions by using a mirror vault

A mirror vault is a repository where Hybrid Backup Recovery (HBR) stores backup data in the cloud. You can use a mirror vault for geo-disaster recovery and cross-region data restoration.

> **Note**
>
> - After a mirror vault is created, the data in the backup vault is synchronized to the mirror vault in real time. The historical backup data stored in the backup vault is 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 data from a mirror vault but cannot back up data to the mirror vault.
> - Before you can delete a backup vault, you must delete its mirror 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.
2. In the left-side navigation pane, click **Overview**.
3. Find the card of the backup vault for which you want to create a mirror vault. In the upper-right corner of the card, click **Cross-Region Backup**.
4. In the Create Mirror Vault dialog box, 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.
   > - All the regions where the mirror vault can reside are displayed in the console.

5. Specify the Vault Name and Description parameters, and then click **Create**.

The vault name must be 1 to 64 characters in length.

Restore data from a mirror vault

If you need to restore data from a mirror vault, log on to the HBR console on an ECS instance. The ECS instance must reside in the same region as the mirror vault. Then, install the backup client. To restore data from a mirror vault, perform the following steps:

1.
2. Install a backup client on an ECS instance.

   > **Note** Select the mirror vault.

3. Restore data to the ECS instance in the HBR console.

   > **Note** Select **Other ECS Instance** or **Local Server** from the **Restore From** drop-down list.

5.7. Use tags

You can use tags to identify resources. Tags allow enterprises and individuals to categorize their ECS resources and simplify the search and management of resources. This topic describes how to use the tag feature for ECS file backup.

Prerequisites

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

Context

You can create different tags for different ECS instances. For example, if you manage teams or projects, you can create tags by 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 ECS instances based on the tag when you maintain ECS instances.

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 by 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.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
3. In the top navigation bar, select a region.
4. On the **ECS File Backup** page, click **New Version**.
5. In the **Tags (Backup Clients)** column, click the  icon next to the name or ID of the ECS instance 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 tag

On the right of the **ECS Assets** tab, select **Client 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:

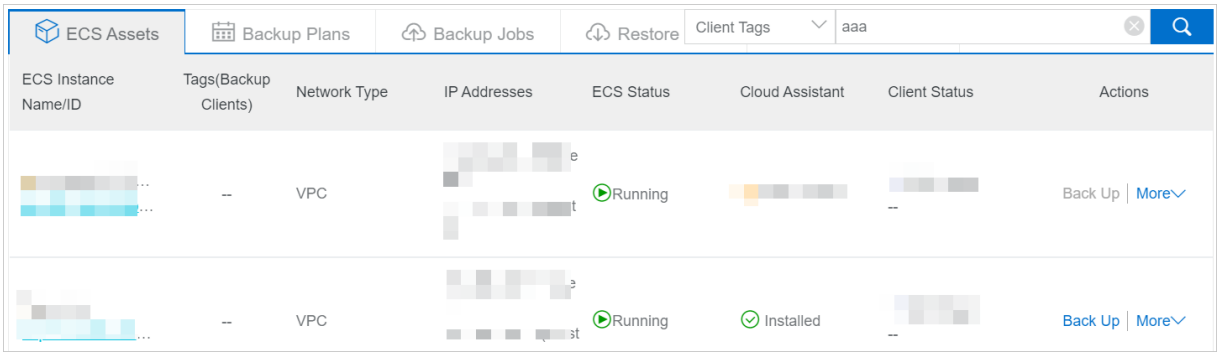
  ```
  aaa
  ```

- 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
  ```


ECS Assets
Backup Plans
Backup Jobs
Restore
Client Tags
aaa
ECS Instance Name/ID
Tags(Backup Clients)
Network Type
IP Addresses
ECS Status
Cloud Assistant
Client Status
Actions
VPC
Running
Back Up
More
VPC
Running
Installed
Back Up
More

6.Earlier versions of ECS file backup

6.1. 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 for Elastic Compute Service (ECS) to back up files from an ECS instance. You can then restore the files when they are lost or damaged. HBR backs up and restores files in streaming mode.

You can use the following procedure to back up files from ECS:

- Prepare for backup
- Back up files from ECS
- Restore backup files

> **Note** For more information, see Back up on-premises files.

6.2. Prepare for a data backup

You can use Hybrid Backup Recovery (HBR) to back up files from Elastic Compute Service (ECS) instances and restore the files based on your requirements. This topic describes how to prepare for a data backup.

Precautions

- To optimize the backup speed, we recommend that you run a backup client on an ECS instance that has the following configurations: 64-bit processors, two or more CPU cores, and more than 8 GB of available memory.
- The volume of data that can be backed up depends on the available memory. If a backup client has 4 GB of available memory, up to one million files or 8 TB of data can be backed up. If you want to back up tens of millions of files, we recommend that you configure 16 GB of available memory for the backup client.

Step 1: Create and assign the AliyunServiceRoleForHbrEcsBackup role

Before you use HBR to back up files from ECS, you must create the AliyunServiceRoleForHbrEcsBackup role and assign the role to HBR. To create and assign the role, perform the following steps:

1.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
   In the dialog box that appears, create and assign the role as prompted.
3. In the **Hybrid Cloud Backup Service Authorization** dialog box, click **Confirm Authorization**.

   For more information, see Service-linked roles.

Step 2: Install Cloud Assistant

An HBR backup client for ECS must be used together with Cloud Assistant.

- If the ECS instance that you need to back up was purchased before December 1, 2017, you must install the Cloud Assistant client. For more information, see Install the Cloud Assistant client.

- If the ECS instance that you need to back up was purchased on or after December 1, 2017, the Cloud Assistant client is pre-installed.

6.3. Install an HBR backup client for ECS

Before you can back up files from an Elastic Compute Service (ECS) instance and restore these files, you must install a backup client on the ECS instance in the Hybrid Backup Recovery (HBR) console.

Background information

You can use the wizard in the HBR console to install backup clients on several ECS instances in the same region. You can also use a template to install backup clients on a large number of or all of the ECS instances in the same region.

If the version of a backup client for ECS is outdated, you can upgrade the client to the latest version. If the activation or upgrade of a backup client for ECS fails, you must uninstall and reinstall the client. If you no longer need the backup data in a backup client for ECS, you can delete the client.

Install backup clients on several ECS instances

To install backup clients on several ECS instances in the same region, perform the following steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
3. In the top navigation bar, select the region where the ECS instances reside.
4. In the upper-right corner of the **ECS Instances** tab, click **Add ECS Instance**.
5. In the **Add ECS Instance** pane, set the parameters. The following table describes the parameters.

Parameter or section	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 a backup vault only 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.

Parameter or section	Description
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 migration or restore job.
ECS instances	In this section, select the ECS instances on which you want to install backup clients. To search for ECS instances, perform the following steps: Select **Instance ID**, **Instance Name**, **VPC ID**, **Private IP (VPC)**, or **Internal IP (Classic)** from the drop-down list next to the search box. Enter a partial or entire keyword in the search box. **Notice** If you select an ECS instance in the classic network, you must provide an AccessKey pair that is used to access the ECS instance. We recommend that you use the AccessKey pair of a RAM user.

6. Click **Create**. HBR then installs a backup client on each selected ECS instance.

Install backup clients on a large number of ECS instances

To install backup clients on a large number of ECS instances in the same region, perform the following steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
3. In the top navigation bar, select the region where the ECS instances reside.
4. In the upper-right corner of the **ECS Instances** tab, choose **Batch Actions > Add ECS Instances**.
5. In the **Add ECS Instances** pane, enter a backup vault name in the **Vault Name** field. The name must be 1 to 64 characters in length.
6. Optional. Select Private IP (VPC) or Internal IP (Classic) . Specify the private or internal IP addresses of the ECS instances on which you want to install backup clients.

   Note
   - By default, the template lists the ECS instances in the region. On these ECS instances, the Cloud Assistant client is installed but the backup client is not installed.
   - If you specify ECS instance IP addresses, the template lists only the specified ECS instances.
   - Separate each IP address with a comma (,).

7. Click **Download Template**.
8. Open the template, specify the **Access Key ID** and **Access Key Secret** fields for ECS instances in the classic network, and then save the template. You do not need to specify AccessKey pairs for VPC ECS instances.

   > **Note**
   > - If you attempt to install backup clients on more than 20 ECS instances by using a template, HBR automatically creates new backup vaults to support the backup clients.
   > - For more information about how to create an AccessKey pair, see View the information about an AccessKey pair.
   > - If you do not need to install a backup client on an ECS instance, delete the row that corresponds to the ECS instance from the template.
   > - We recommend that you do not change the values in the **Instance Id**, **Instance Name**, and **Network Type** columns.
   > - To ensure account security, we recommend that you delete the local template after the template is uploaded to HBR.

9. Click **Upload Template**.

   After the template is uploaded, the number of VPC ECS instances and the number of classic network ECS instances are displayed.

Manage a backup client

On the **ECS Instances** tab of the **ECS File Backup** page, find the ECS instance that hosts the backup client. To search for an ECS instance, select Private IP (VPC) or Internal IP (Classic) from the drop-down list next to the search box, enter the IP address of the ECS instance, and then click the Search icon.

You can view the installation status of the backup client. After the backup client is installed, you can uninstall, delete, or upgrade the backup client.

Operation	Description
Check the installation status of the backup client	If the backup client is installed, the client status is Activated . If the client status is Installation Failed , it indicates that the installation of a backup client fails. Follow the instructions in the error message to troubleshoot the error. After the error is fixed, choose **More > Install Client** in the **Actions** column.
Uninstall the backup client	Choose **More > Uninstall Client** in the **Actions** column.
Delete the backup client	To uninstall the backup client from the ECS instance and remove the ECS instance, choose **More > Remove** in the **Actions** column. **Note** After you delete a backup client, the existing backup data is also deleted and running backup and restore jobs fails. Before you delete a backup client, make sure that the backup data in the client is no longer needed and the client has no running backup or restore jobs.

Operation	Description
Upgrade the backup client to the latest version	Click **Upgrade** in the Client Type column.

6.4. Back up files from ECS instances

You can use Hybrid Backup Recovery (HBR) to back up files from Elastic Compute Service (ECS) and restore the files if needed. This topic describes how to back up files from ECS instances.

Prerequisites

Preparations are completed.

Back up files from an ECS instance

To back up files from an ECS instance, perform the following steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
3. On the **ECS File Backup** page, click the **ECS Instances** tab.
4. On the ECS Instances tab, find the ECS instance and click **Back Up** in the Actions column.
5. In the **Create Backup Plan** pane, set the parameters and click **OK**. The following table describes the parameters.

Parameter	Description
Plan Name	The name of the backup plan. By default, a random name is used.

Parameter	Description
Source Paths	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 the files to be excluded from the backup plan. ○ If UNC paths are used, VSS backup and wildcards (*) are not supported. You cannot specify the files to be excluded from the backup plan. If a UNC path is specified, HBR does not back up the access control list (ACL) of Windows.

Parameter	Description
Backup Rule	The rule that specifies the files to be excluded from the backup plan. Select **Include All Files** or **Exclude Specified Files**. If you select **Exclude Specified 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 (\).
Start Time	The start time of the backup plan. The time is accurate to seconds.
Backup Interval	The interval at which data backup is performed. Unit: hours, days, or weeks. **Note** The maximum interval is 52 weeks (1 year).
Retention Period	The retention period of the backup data. Unit: days, weeks, months, or years.
Use VSS	◦ Specifies whether to use Volume Shadow Copy Service (VSS) for backup. This parameter is valid only for Windows ECS instances. ◦ If data in the backup source changes, select **Yes**. VSS ensures data consistency between the source and the backup. ◦ 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.

Parameter	Description
Throttle Bandwidth	Specifies whether to throttle the bandwidth. You can throttle the bandwidth that is used for data backup during peak hours. This guarantees business continuity. If you select **Yes**, you must set the Throttling Period (Hour) and Max Bandwidth parameters. Then, click **Add**.

Back up files from multiple ECS instances

You can create multiple backup plans back up files from multiple ECS instances. To create multiple backup plans in a batch, perform the following steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
3. In the top navigation bar, select the region where the ECS instances reside.
4. In the upper-right corner, choose **Batch Actions > Create Backup Plans**.
5. In the **Create Backup Plans** pane, click **Download Template**.
6. Open the template, set the parameters, and then save the template. The following table describes the parameters.

> **Note** If you do not need to back up files from an ECS instance, delete the row that corresponds to the ECS instance from the template.

Parameter	Description
Client Id	The ID of the backup client. Do not change the client ID.
Instance Id	The ID of the ECS instance where the backup client is installed. Do not change the instance ID.
Instance Name	The name of the ECS instance where the backup client is installed. Do not change the instance name.
Source	The path to the directory from which you want to back up files. The path must be an absolute path.
Plan Name	The name of the backup plan. If you do not specify this parameter, a random name is used.
Retention (Day)	○ The retention period of backup data. Enter an integer. ○ Unit: days. ○ If you do not specify this parameter, the backup data is retained for 730 days.

Parameter	Description
Effective Time	The start time of the backup plan. Specify the time in the `YYYY-MM-DD/HH:MM:SS` format, for example, 2018-12-03/12:00:00.
Backup Interval	○ The interval at which incremental backup is performed. Enter an integer. ○ Unit: hours. ○ If you do not specify this parameter, the interval is 24 hours.
Use VSS for backup	○ This feature is only available for Windows ECS instances. ○ If data in the backup source changes, enable this feature. VSS ensures data consistency between the source and the backup. ○ Enter *Y* to enable this feature or *N* to disable this feature. If you do not specify this parameter, the feature is disabled. ○ If you use VSS, you cannot back up data from multiple directories.
Bandwidth Throttling	○ Specifies whether to throttle the bandwidth. You can throttle the bandwidth that is used for data backup. This guarantees business continuity. ○ If you enable this feature, specify the maximum bandwidth that can be used for backup. The maximum bandwidth applies all day. ○ Enter an integer. Unit: MB/s. ○ If you do not specify this parameter, the bandwidth is not throttled.

7. Click **Upload Template** to upload the template.
8. Click **OK**.

Query files that are backed up

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

1. On the **Backup Plans and Jobs** tab, find the backup plan, and click **View** 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 to an ECS instance.

What to do next

On the **ECS File Backup** page, click the **Backup Plans and Jobs** tab. On this tab, you can perform the following operations on a backup plan.

Operation	Procedure
View an error report	Find the backup plan and view the backup progress in the Status column. If the backup of some files fail, click **View** in the Actions column. In the Errors column, click the **Download** icon to download the error report.
Start a backup job	Find the backup plan, and choose **More** > **Run Immediately** in the **Actions** column.
Cancel a running backup job	Find the backup plan, and choose **More** > **Cancel Job** in the **Actions** column.
Pause a running backup job	Find the backup plan, and choose **More** > **Suspend** in the **Actions** column.
Resume a paused backup job	Find the backup plan, and choose **More** > **Resume** in the **Actions** column.
Modify a backup plan	Find the backup plan, and choose **More** > **Modify** in the **Actions** column.
Delete a backup plan	Find the backup plan, and choose **More** > **Delete** in the **Actions** column. After you delete the backup plan, HBR no longer runs backup jobs for the plan but the backup data is retained.

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
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.

Parameter	Description
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
```

6.5. Restore files to an ECS instance

You can restore files to an Elastic Compute Service (ECS) instance from a backup of the same ECS instance or another ECS instance that uses the same backup vault. You can also restore files to an ECS instance from a backup of an on-premises client. You can also use a mirror vault to restore files to an ECS instance in a different region or use a local backup client to restore files to the current ECS instance.

Prerequisites

Files are backed up from ECS instances. For more information, see Back up files from ECS instances.

Restore files to an ECS instance in the same region as the source ECS instance

To restore files to an ECS instance in the same region as the source ECS instance, perform the following steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
3. On the **ECS File Backup** page, click the **ECS Instances** tab.
4. On the ECS Instances tab, find the destination ECS instance, and click **Restore** in the **Actions** column.
5. In the **Create Restore Job** pane, set the Restore From parameter to one of the following values:
   - **Current ECS Instance**

     Select this option if you need to restore files from the current ECS instance. Then, perform the following steps:

     a. Click **Next**.

     b. In the Select Backup step, select a backup and click **Next**.

c. In the **Configure Restore Policy** step, enter a destination path, select a restore policy, specify the files that you want to restore based on the policy, and then click **Create**.

To specify the files to restore, you can select files or enter a list of paths to directories and files.

Select one of the following options as the restore policy:

- **Include All Files**: HBR restores all files that are backed up from the source ECS instance.
- **Include Specified Files** or **Exclude Specified Files**: In the text box, enter the paths to the directories and files that you want to restore. HBR restores files that are backed up from the source ECS instance based on the restore policy.

In the text box, enter one path in each line and start each path with the source directory.

If the source path is C:\Windows\ABC and you want to restore folder and folder\file.txt in the ABC directory, enter the following paths:

```
\ABC\folder \ABC\folder\file.txt
```

- **Other ECS Instance**

Select this option if you need to restore files from another ECS instance that uses the same backup vault as the current ECS instance. Then, perform the following steps:

a. Select the source ECS instance and click **Next**.

b. In the Select Backup step, select a backup and click **Next**.

c. In the **Configure Restore Policy** step, enter a destination path, select a restore policy, specify the files that you want to restore based on the policy, and then click **Create**.

> **Note** The method to configure a restore policy for data restoration from another ECS instance is the same as the method to configure a restore policy for data restoration from the current ECS instance.

- **On-premises Server**

Select this option if you need to restore files from an on-premises server. Then, perform the following steps:

a. Select the client that is used to back up the files from the on-premises server and click **Next**.

b. In the Select Backup step, select a backup and click **Next**.

c. In the **Configure Restore Policy** step, enter a destination path, select a restore policy, specify the files that you want to restore based on the policy, and then click **Create**.

> **Note** The method to configure a restore policy for data restoration from an on-premises server is the same as the method to configure a restore policy for data restoration from the current ECS instance.

> **Note** You can view the progress of the created restore job on the **Restore Jobs** tab of the **ECS File Backup** page.

Restore files to an ECS instance in a different region from the source ECS instance

A backup vault is a repository that HBR uses to store backup data in the cloud. A mirror vault is the mirror of a backup vault. The two vaults reside in different regions. You can restore files of ECS instances across regions by using a mirror vault to implement disaster recovery.

Before you can restore files to an ECS instance in another region, you must create a mirror vault for the backup vault of the source ECS instance. For information about how to create a mirror vault, see Back up data across regions.

To restore files to an ECS instance in another region, perform the following steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
3. Select the region where the mirror vault resides.
4. On the **ECS Instances** tab, install a backup client on the destination ECS instance.

   > **Note** You must select an existing mirror vault. Mirror vaults are tagged with [COPY]. For more information about how to set other parameters when installing the backup client, see Install backup clients on several ECS instances.

5. Click **Restore** in the Actions column.

   Select **Other ECS Instance** or **On-premises Server** as **Restore From**. For information about how to set the other parameters, see Restore files to an ECS instance in the same region as the source ECS instance.

6.6. Configure alert notifications

HBR sends alert notifications to the Alibaba Cloud account owner by default when backup fails or a backup client is disconnected from HBR. You can customize notification contacts, contact groups, and methods.

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

Create a notification contact

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

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

   After you select Email, enter an email address in the **Email** field and click **Send**. Log on to the specified email address and copy the verification code. Then, paste the code in the Verification

Code field in the HBR console.

7. Click **OK**.

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

Create a contact group

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

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

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

Create alert policies

You can create the following types of alarm policies:

> **Note** By default, HBR sends alert notifications by using emails to the Alibaba Cloud account owner. If you use custom alert policies, an instance-level alert policy takes precedence over a vault-level alert policy.

- Vault-level alert policy

  A vault-level alert policy applies to all the backup clients that are associated with the vault. The backup clients include those for ECS, on-premises files, and on-premises virtual machines (VMs).

To configure an alert policy for a vault, perform the following steps:

i. Log on to the HBR console.
ii. On the **Overview** page, find the vault.
iii. In the upper-right corner of the vault card, click the Settings icon.
iv. In the **Modify Backup Vault** pane, select an alert policy based on your requirements.

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

v. Click **OK**.

- Instance-level alert policy

  An instance-level alert policy applies to the backup client of an ECS instance.

  To configure an alert policy for an ECS instance, perform the following steps:

  i. Log on to the HBR console.
  ii. Find the ECS instance. In the Actions column, choose > **Alert Settings**.
  iii. In the **Alert Settings** pane, select an alert policy based on your requirements.

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

  iv. Click **OK**.

6.7. Use tags

You can use tags to identify resources. You can use tags to categorize your ECS resources. This way, you can search and manage resources in a more efficient way. This topic describes how to use the tagging feature to back up ECS files.

Prerequisites

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

Context

You can create different tags for different ECS instances. 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 ECS instances based on the tag when you maintain ECS instances.

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.
2. In the left-side navigation pane, choose **Backup > ECS File Backup**.
3. In the top navigation bar, select a region.
4. On the **ECS File Backup** page, click **Old Version**.
5. In the **Tags** column, click the  icon next to the name or ID of the ECS instance 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 resources by tag

On the right side of the **ECS Instances** 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
  ```