Alibaba Cloud Hybrid Backup

ECS Disaster Recovery

Issue: 20200623

Legal disclaimer

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the 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 contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
	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.
	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.
	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.
	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]`

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	switch {active|stand}

Contents

1 What is ECS Disaster Recovery?

Elastic Compute Service (ECS) Disaster Recovery is a scheme provided by Alibaba Cloud Hybrid Backup Recovery (HBR) to serve the needs of key enterprise applications and guarantee business continuity. It features disaster recovery with a second-level or minute-level recovery point objective (RPO) and recovery time objective (RTO).

Scenarios

ECS Disaster Recovery can be used across regions and zones in the following two scenarios :

- The primary and disaster recovery systems are deployed in different regions of Alibaba Cloud. When the primary system encounters a failure, the business system switches to the disaster recovery system. By deploying the primary and disaster recovery systems in different regions, ECS Disaster Recovery provides a highly reliable and disaster recovery-based service. This service features an RPO of as low as 1 minute and an RTO of as low as 15 minutes. Cross-region disaster recovery can guarantee business continuity and effectively avoid system failures caused by regional disasters. For more information, see Cross-region disaster recovery.
- When a production site encounters force majeure events such as a fire disaster or an earthquake or equipment failures such as software or hardware failures, applications may fail to run in a certain period. In this case, ECS Disaster Recovery provides cross-zone disaster recovery for you to back up application data and run applications in another zone to deal with failures in a single zone at the required RTO and RPO. For more information, see Cross-zone disaster recovery.

Main capabilities

ECS Disaster Recovery provides the following capabilities:

- Application data replication in real time: ECS Disaster Recovery can monitor data changes in disks of operating systems and ECS instances, capture changed data, and then synchronize such data to disaster recovery sites in real time. In this way, it provides real-time protection for your data with a second-level or minute-level RPO.
- Quick application running in another region or zone: You can quickly run applications in another region or zone within minutes.

- Disaster recovery drills without business interruption: You can perform disaster recovery drills on application servers deployed on the cloud at any time to verify the business restorability. Disaster recovery drills do not affect the source production environment or interrupt data replication.

Benefits

ECS Disaster Recovery has the following benefits:

- Cost-effective: ECS Disaster Recovery consumes only disk resources and a small number of computing resources. It only requires software authorization such as authorization from operating and application systems during disaster recovery.
- Easy to use: You can start data replication for disaster recovery, perform disaster recovery drills, and restore data in one click without deploying a disaster recovery center .
- Highly reliable: ECS Disaster Recovery can guarantee continuous data replication and resumable upload even when errors occur, for example, the source server is overloaded or restarted, the disaster recovery gateway is restarted upon power-off, or the data replication link encounters network jitter. Alibaba Cloud guarantees the reliability of cloud data.
- Highly secure: ECS Disaster Recovery uses the Advanced Encryption Standard (AES) 256-bit algorithm and HTTPS to encrypt your data and guarantee end-to-end security.
- Verifiable: You can perform disaster recovery drills on cloud systems at any time without affecting the production system. This overcomes the difficulties in verifying the disaster recovery system.

2 Service linked role for ECS disaster recovery

This topic describes the AliyunServiceRoleForHbrDr service linked role and how to delete the role. This role is used for Elastic Compute Service (ECS) disaster recovery.

Background information

In some cases, Hybrid Backup Recovery may need to access resources from other cloud services to implement a disaster recovery-related feature. To meet the need, Alibaba Cloud offers a Resource Access Management (RAM) role named AliyunServiceRoleForHbrDr. For more information about service linked roles, see #unique_7.

In the Hybrid Backup Recovery console, you may need to create new VSwitches, security groups, Elastic Compute Service (ECS) instances, images, and other resources. You can use the AliyunServiceRoleForHbrDr service linked role to access Virtual Private Cloud (VPC) and ECS resources.

Introduction

Role name: AliyunServiceRoleForHbrDr

Policy name: AliyunServiceRolePolicyForHbrDr

Policy document:

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "ecs:DescribeImages",
        "CreateDisk",
        "ecs:AttachDisk",
        "ecs:ReInitDisk",
        "ecs:DetachDisk",
        "ecs:DescribeDisks"
        "ecs:ReplaceSystemDisk",
        "ecs:DeleteDisk",
        "ecs:ResizeDisk",
        "ecs:CreateInstance",
        "ecs:StartInstance",
        "ecs:StopInstance",
        "ecs:RebootInstance",
        "ecs:DeleteInstance",
        "ecs:DescribeInstances",
        "ecs:CreateSecurityGroup",
        "ecs:DescribeSecurityGroups",
        "ecs:AuthorizeSecurityGroup",
        "Action": "ecs:AuthorizeSecurityGroupEgress",
        "ecs:DeleteSecurityGroup",
        "ecs:AllocatePublicIpAddress",
        "ecs:ModifyInstanceAttribute",
```

```
      "ecs:JoinSecurityGroup",
      "ecs:CreateNetworkInterface",
      "ecs:DeleteNetworkInterface",
      "ecs:DescribeNetworkInterfaces",
      "ecs:CreateNetworkInterfacePermission"
      "ecs:DescribeNetworkInterfacePermissions",
      "ecs:DeleteNetworkInterfacePermission",
      "ecs:CreateSnapshot",
      "hbr:DeleteSnapshot"
      "ecs:DescribeSnapshots",
      "ecs:DescribeSnapshotLinks",
      "ecs:CreateCommand",
      "ecs:InvokeCommand",
      "ecs:StopInvocation",
      "ecs:DeleteCommand",
      "ecs:DescribeCommands",
      "ecs:DescribeInvocations",
      "ecs:DescribeInvocationResults",
      "ecs:DescribeCloudAssistantStatus",
      "ecs:ModifyResourceMeta"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "vpc:DescribeVpcs",
      "vpc:DescribeVSwitches",
      "vpc:DescribeEipAddresses"
      vpc:AssociateEipAddress
    ],
    "Resource": "*",
    "Effect": "Allow"
  }
 ]
}
```

Delete the AliyunServiceRoleForHbrDr role

Before you delete the AliyunServiceRoleForHbrDr service linked role, you must remove all site pairs on the Cloud Disaster Recovery page of the Hybrid Backup Recovery console.

For more information about how to delete a service linked role, see #unique_7/unique_7_Connect_42_section_b9f_8dv_b5q.

3 Limits

This topic describes the limits for Elastic Compute Service (ECS) Disaster Recovery, including the limits on operating systems, architectures, databases, and applications.

Operating systems

The following table lists the operating systems that support ECS Disaster Recovery.

Operating system	Version
Windows Server	2008 R2, 2012, 2012 R2, and 2016
Linux	• Red Hat Enterprise Linux 7.0#7.8 • Red Hat Enterprise Linux 6.0#6.10 • CentOS 7.0#7.8 • CentOS 6.0#6.10 **Note:** ECS Disaster Recovery is supported on servers that run CentOS 6.x 64-bit operating systems. To support ECS Disaster Recovery on servers that run CentOS 6.x 32-bit operating systems, contact the technical support staff. • SUSE Linux Enterprise Server 12.0#12.3 **Notice:** ECS Disaster Recovery is supported on servers that run SUSE Linux Enterprise Server 12.x 64-bit operating systems. To support ECS Disaster Recovery on servers that run SUSE Linux Enterprise Server 12.x 32-bit operating systems, contact the technical support staff. When SUSE Linux Enterprise Server 12.1 runs on a VMware virtual machine, a black screen appears after the virtual machine is restarted. This is caused by system errors of the operating system, irrelevant to ECS Disaster Recovery.

Note:
ECS Disaster Recovery will be supported in more Linux versions in the near future.

Architectures

ECS Disaster Recovery is implemented based on the disk-level data replication. It is independent of the underlying architecture. The following table lists the platforms that support ECS Disaster Recovery. More platforms that support ECS Disaster Recovery are being verified. If you have any questions, contact the technical support staff.

Architecture	Version
Physical machine	Full support
Hyper-V	2008 R2, 2012, and 2012 R2
vSphere	5.5, 6.0, and 6.5

Databases and applications

The replication technology of ECS Disaster Recovery can be applied to all types of databases and applications.

In most cases, automated scripts are required for various applications to keep consistenc y among updates. When you perform ECS Disaster Recovery, you can use the available tools provided by Alibaba Cloud along with the scripts to guarantee smooth recovery of applications.

Other limits

ECS Disaster Recovery also has the following limits:

- If the size of a volume where a system disk of an ECS instance resides exceeds 2 TB, you cannot perform a full restoration on the ECS instance.
- A single physical volume of a data disk cannot exceed 32 TB.

4 Cross-region disaster recovery

The primary and disaster recovery systems are deployed in different regions of Alibaba Cloud. When the primary system encounters a failure, the business system switches to the disaster recovery system. By deploying the primary and disaster recovery systems in different regions, Elastic Compute Service (ECS) Disaster Recovery provides a highly reliable and disaster recovery-based service. This service features a recovery point objective (RPO) of as low as 1 minute and a recovery time objective (RTO) of as low as 15 minutes. Cross-region disaster recovery can guarantee business continuity and effectively avoid system failures caused by regional disasters.

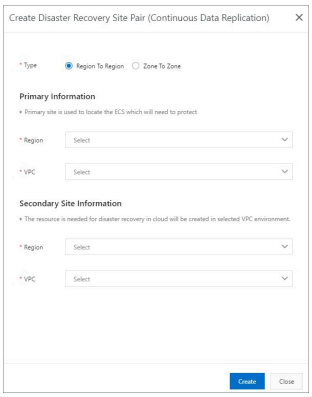
Preparations

Before you implement cross-region disaster recovery, you must select a region different from that of the production environment as the destination region, create a Virtual Private Cloud (VPC) in the destination region, and then create a VSwitch separately for the replication and restoration networks in the VPC.

Step 1: Create a disaster recovery site pair

To create a disaster recovery site pair to provide cross-region disaster recovery protection for ECS instances in the primary site, follow these steps:

1. Log on to the Hybrid Backup Recovery (HBR) console.
2. In the left-side navigation pane, choose **Disaster Recovery** > **ECS Disaster Recovery**.
3. On the **Site Pair Information** tab, click **Add** in the upper-right corner.
4. In the **Create Disaster Recovery Site Pair (Continuous Data Replication)** pane that appears, set Type to **Region To Region** and select the region and VPC for the primary and secondary sites.



5. Click **Create**.

Step 2: Add the ECS instances to be protected

To add the ECS instances to be protected, follow these steps:

1. Click the **Protected Server** tab. On this tab, select the disaster recovery site pair you create in step 1 from the drop-down list in the upper-right corner.
2. On the Protected Server tab, click **Add**. In the Add Protected Server pane that appears, select at least one ECS instance to be protected and click **OK**.

   You can select a maximum of 10 ECS instances.

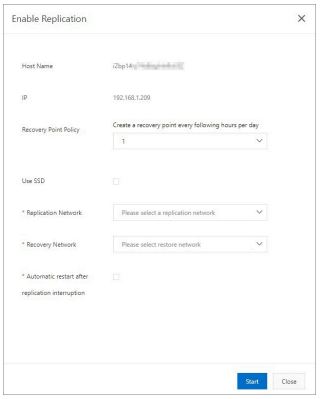
   Verify that the status of one or more added ECS instances in the Server Status column is Agent Installing and then changes to Initialized. If the status of an ECS instance is not Initialized, choose **More** > **Server Operation** > **Restart Server** in the Operation column to initialize the instance.

Step 3: Start replication

To replicate ECS instances to the cloud and maintain real-time replication, follow these steps:

1. On the **Protected Server** tab, find the ECS instance to be replicated and choose **More** > **Failover** > **Start Replication** in the **Operation** column.
2. In the **Enable Replication** pane that appears, set **Recovery Point Policy**, **Use SSD**, **Replication Network**, **Recovery Network**, and **Automatic restart after replication interruption**.

   Note:
   The VSwitches used for the replication and restoration networks must be in the same zone.



3. Click **Start**.

   Then, the ECS instance enters the **Enable Replicating**, **Initial Full Sync**, and **Replicating** states in sequence.

   - **Enable Replicating**: ECS Disaster Recovery is scanning data on the ECS instance and evaluating the overall data volume. This process usually lasts a few minutes.
   - **Initial Full Sync**: ECS Disaster Recovery is replicating valid data on the ECS instance to Alibaba Cloud. The replication duration depends on factors such as the volume of valid data on the instance and the network bandwidth. The progress bar in the Server Status column shows the replication progress.
   - **Replicating**: After all valid data on the ECS instance is replicated to Alibaba Cloud through full replication, Aliyun Replication Service (AReS) monitors all write operations performed on disks on the ECS instance and continuously replicates incremental data to Alibaba Cloud in real time.

(Optional) Perform a disaster recovery drill

After an ECS instance enters the Replicating state, you can perform a disaster recovery drill on the ECS instance.

A disaster recovery drill is an important part of disaster recovery. It allows you to run a protected ECS instance on the cloud to verify the correctness of relevant applications. It has the following core features:

- Allows you to easily check whether a protected application can be run on the cloud.
- Helps you be familiar with the disaster recovery process and makes sure that you can smoothly perform failover when the primary site encounters a failure.

To perform a disaster recovery drill, follow these steps:

1. On the **Protected Server** tab, find the target ECS instance and click **Disaster Recovery Drill** in the **Operation** column.
2. In the **Test Failover** pane that appears, set **Recovery Network**, **IP Address**, **Use ECS Specification**, **Hard Disk Type**, **Recovery Point**, **Elastic Public Network IP**, and **Execute script after failover**.

   Note:

   - HBR automatically retains 24 recovery points in the last 24 hours for each ECS instance.

- If you do not select Use ECS Specification, you must specify the number of vCPUs and memory capacity.

3. Click **Start**.

   Then, Alibaba Cloud runs the ECS instance in the background at the specified time. The disaster recovery drill performed in the background does not affect real-time data replication.

4. After the disaster recovery drill is completed within a few minutes, click the link in the **Disaster Recovery Information** column to verify restored data and applications.

5. After the verification is completed, click **Clear Test Failover Environment** in the **Operation** column. Then, the restored ECS instance is deleted.

   Note:
   After the restored ECS instance is verified, we recommend that you delete the restored ECS instance as soon as possible to reduce costs.

Step 4: Perform failover

Regular disaster recovery drills make sure that you can run your business on the cloud at any time. When a major error occurs in the primary site, you may need to restart your core business on the cloud immediately. In this case, you must perform failover.

Warning:
Failover is applicable to protected ECS instances where a serious error occurs. During the failover, ECS Disaster Recovery stops real-time data replication. To resume protection for a protected ECS instance, you must restart data replication and replicate all valid data on the ECS instance to Alibaba Cloud again.

To perform failover, follow these steps:

1. On the **Protected Server** tab, find the target ECS instance and choose **More** > **Failover** > **Failover** in the **Operation** column.
2. In the **Failover** pane that appears, set **Recovery Network**, **IP Address**, **Use ECS Specification**, **Hard Disk Type**, **Recovery Point**, **Elastic Public Network IP**, and **Execute script after failover**.

   Notice:
   You can restore the ECS instance to the current point in time only once.

3. Click **Start**.
4. After the failover is completed, click the link in the **Recovered Instance ID/Name** column to verify restored data and applications.
   - If the applications run properly after being restored to the current point in time, choose **More** > **Failover** > **Commit Failover** in the Operation column.

     Note:
     After you complete the failover or change the recovery point and verify that applications restored from the protected ECS instance are running your business, you can commit the failover to release the cloud resources occupied during failover to save resources.
   - If the applications do not meet the requirements after being restored to the current point in time, for example, data in the restored database is inconsistent with that in the source database, or dirty data on the source ECS instance is synchronized to the restored ECS instance in the destination region, choose **More** > **Failover** > **Change Recovery Point** in the Operation column to change the recovery point before you commit the failover.

     Note:
     The procedure for changing the recovery point is similar to that for failover, except that you must select a recovery point earlier than the current point in time.

Step 5: Perform reverse replication

After you replicate applications on a protected ECS instance in a region like Region A to another region like Region B, you can also perform reverse replication to replicate applications from Region B to Region A.

To perform reverse replication, follow these steps:

1. On the **Protected Server** tab, find the target ECS instance and choose **More** > **Failback** > **Reversed Register** in the **Operation** column. In the message that appears, confirm that you want to perform reverse registration on the ECS instance.
2. Choose **More** > **Failback** > **Initiate Reverse Replication** in the **Operation** column.

3. In the **Initiate Reverse Replication** pane that appears, set **Original machine recovery**, **Replication Network**, and **Recovery Network**.

    **Warning:**

   Cross-region disaster recovery and cross-zone disaster recovery allow you to replicate applications back to the original ECS instance. However, when you replicate applications back to the original ECS instance, data on the original ECS instance is overwritten. Perform this operation with caution.

4. Click **Start**.
5. After the ECS instance enters the Reversed Enable Replicating state, choose **More** > **Failback** > **Failback** in the **Operation** column.
6. In the **Failback** pane that appears, set **CPU**, **Memory**, **Recovery Network**, **IP Address**, and **Execute script after recovery**, and click Start.
7. After the failback is completed, choose **More** > **Failover** > **Registration** in the **Operation** column to register the protected ECS instance again.

5 Cross-zone disaster recovery

When a production site encounters force majeure events such as a fire disaster or an earthquake or equipment failures such as software or hardware failures, applications may fail to run in a certain period. In this case, Elastic Compute Service (ECS) Disaster Recovery provides cross-zone disaster recovery for you to back up application data and run applications in another zone to deal with failures in a single zone at the required recovery time objective (RTO) and recovery point objective (RPO).

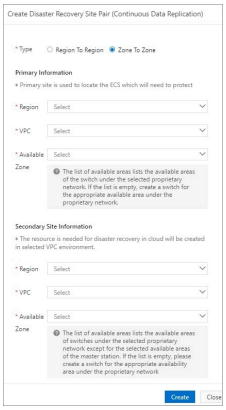
Preparations

Before you implement cross-zone disaster recovery, you must select a zone different from that of the production environment as the destination zone, create a Virtual Private Cloud (VPC) in the destination zone, and then create a VSwitch separately for the replication and restoration networks in the VPC.

Step 1: Create a disaster recovery site pair

To create a disaster recovery site pair to provide cross-zone disaster recovery protection for ECS instances in the primary site, follow these steps:

1. Log on to the Hybrid Backup Recovery (HBR) console.
2. In the left-side navigation pane, choose **Disaster Recovery** > **ECS Disaster Recovery**.
3. On the **Site Pair Information** tab, click **Add** in the upper-right corner.
4. In the **Create Disaster Recovery Site Pair (Continuous Data Replication)** dialog box that appears, set Type to **Zone To Zone** and select the region, VPC, and zone for the primary and secondary sites.



5. Click **Create**.

Step 2: Add the ECS instances to be protected

To add the ECS instances to be protected, follow these steps:

1. Click the **Protected Server** tab. On this tab, select the disaster recovery site pair you create in step 1 from the drop-down list in the upper-right corner.
2. On the Protected Server tab, click **Add**. In the Add Protected Server pane that appears, select at least one ECS instance to be protected and click **OK**.

   You can select a maximum of 10 ECS instances.

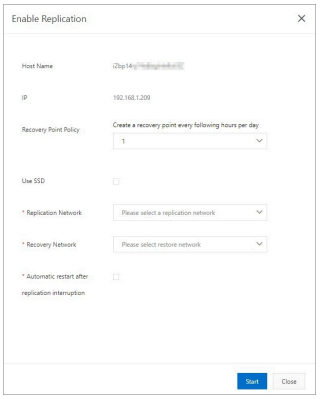
   Verify that the status of one or more added ECS instances in the Server Status column is Agent Installing and then changes to Initialized. If the status of an ECS instance is not Initialized, choose **More** > **Server Operation** > **Restart Server** in the Operation column to initialize the instance.

Step 3: Start replication

To replicate ECS instances to the cloud and maintain real-time replication, follow these steps:

1. On the **Protected Server** tab, find the ECS instance to be replicated and choose **More** > **Failover** > **Start Replication** in the **Operation** column.
2. In the **Enable Replication** pane that appears, set **Recovery Point Policy**, **Use SSD**, **Replication Network**, **Recovery Network**, and **Automatic restart after replication interruption**.

   Note:
   The VSwitches used for the replication and restoration networks must be in the same zone.



3. Click **Start**.

   Then, the ECS instance enters the **Enable Replicating**, **Initial Full Sync**, and **Replicating** states in sequence.

   - **Enable Replicating**: ECS Disaster Recovery is scanning data on the ECS instance and evaluating the overall data volume. This process usually lasts a few minutes.
   - **Initial Full Sync**: ECS Disaster Recovery is replicating valid data on the ECS instance to Alibaba Cloud. The replication duration depends on factors such as the volume of valid data on the instance and the network bandwidth. The progress bar in the Server Status column shows the replication progress.
   - **Replicating**: After all valid data on the ECS instance is replicated to Alibaba Cloud through full replication, Aliyun Replication Service (AReS) monitors all write operations performed on disks on the ECS instance and continuously replicates incremental data to Alibaba Cloud in real time.

(Optional) Perform a disaster recovery drill

After an ECS instance enters the Replicating state, you can perform a disaster recovery drill on the ECS instance.

A disaster recovery drill is an important part of disaster recovery. It allows you to run a protected ECS instance on the cloud to verify the correctness of relevant applications. It has the following core features:

- Allows you to easily check whether a protected application can be run on the cloud.
- Helps you be familiar with the disaster recovery process and makes sure that you can smoothly perform failover when the primary site encounters a failure.

To perform a disaster recovery drill, follow these steps:

1. On the **Protected Server** tab, find the target ECS instance and click **Disaster Recovery Drill** in the **Operation** column.
2. In the **Test Failover** pane that appears, set **Recovery Network**, **IP Address**, **Use ECS Specification**, **Hard Disk Type**, **Recovery Point**, **Elastic Public Network IP**, and **Execute script after failover**.

   Note:

   - HBR automatically retains 24 recovery points in the last 24 hours for each ECS instance.

- If you do not select Use ECS Specification, you must specify the number of vCPUs and memory capacity.

3. Click **Start**.

   Then, Alibaba Cloud runs the ECS instance in the background at the specified time. The disaster recovery drill performed in the background does not affect real-time data replication.

4. After the disaster recovery drill is completed within a few minutes, click the link in the **Disaster Recovery Information** column to verify restored data and applications.

5. After the verification is completed, click **Clear Test Failover Environment** in the **Operation** column. Then, the restored ECS instance is deleted.

   Note:
   After the restored ECS instance is verified, we recommend that you delete the restored ECS instance as soon as possible to reduce costs.

Step 4: Perform failover

Regular disaster recovery drills make sure that you can run your business on the cloud at any time. When a major error occurs in the primary site, you may need to restart your core business on the cloud immediately. In this case, you must perform failover.

Warning:
Failover is applicable to protected ECS instances where a serious error occurs. During the failover, ECS Disaster Recovery stops real-time data replication. To resume protection for a protected ECS instance, you must restart data replication and replicate all valid data on the ECS instance to Alibaba Cloud again.

To perform failover, follow these steps:

1. On the **Protected Server** tab, find the target ECS instance and choose **More** > **Failover** > **Failover** in the **Operation** column.
2. In the **Failover** pane that appears, set **Recovery Network**, **IP Address**, **Use ECS Specification**, **Hard Disk Type**, **Recovery Point**, **Elastic Public Network IP**, and **Execute script after failover**.

   Notice:
   You can restore the ECS instance to the current point in time only once.

3. Click **Start**.
4. After the failover is completed, click the link in the **Recovered Instance ID/Name** column to verify restored data and applications.
   - If the applications run properly after being restored to the current point in time, choose **More** > **Failover** > **Commit Failover** in the Operation column.

     Note:
     After you complete the failover or change the recovery point and verify that applications restored from the protected ECS instance are running your business, you can commit the failover to release the cloud resources occupied during failover to save resources.
   - If the applications do not meet the requirements after being restored to the current point in time, for example, data in the restored database is inconsistent with that in the source database, or dirty data on the source ECS instance is synchronized to the restored ECS instance in the destination region, choose **More** > **Failover** > **Change Recovery Point** in the Operation column to change the recovery point before you commit the failover.

     Note:
     The procedure for changing the recovery point is similar to that for failover, except that you must select a recovery point earlier than the current point in time.

Step 5: Perform reverse replication

After you replicate applications on a protected ECS instance in a zone like Zone A to another zone like Zone B, you can also perform reverse replication to replicate applications from Zone B to Zone A.

To perform reverse replication, follow these steps:

1. On the **Protected Server** tab, find the target ECS instance and choose **More** > **Failback** > **Reversed Register** in the **Operation** column. In the message that appears, confirm that you want to perform reverse registration on the ECS instance.
2. Choose **More** > **Failback** > **Initiate Reverse Replication** in the **Operation** column.

3. In the **Initiate Reverse Replication** pane that appears, set **Original machine recovery**, **Replication Network**, and **Recovery Network**.

    **Warning:**

   Cross-region disaster recovery and cross-zone disaster recovery allow you to replicate applications back to the original ECS instance. However, when you replicate applications back to the original ECS instance, data on the original ECS instance is overwritten. Perform this operation with caution.

4. Click **Start**.
5. After the ECS instance enters the Reversed Enable Replicating state, choose **More** > **Failback** > **Failback** in the **Operation** column.
6. In the **Failback** pane that appears, set **CPU**, **Memory**, **Recovery Network**, **IP Address**, and **Execute script after recovery**, and click Start.
7. After the failback is completed, choose **More** > **Failover** > **Registration** in the **Operation** column to register the protected ECS instance again.