ALIBABA CLOUD

Alibaba Cloud

Hybrid Backup
Disaster Recovery

Document Version: 20220526

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.ECS disaster recovery

1.1. What is ECS disaster recovery?

Elastic Compute Service (ECS) disaster recovery is a scheme that Alibaba Cloud Hybrid Backup Recovery (HBR) provides 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, workloads are switched to the disaster recovery system. By deploying the primary and disaster recovery systems in different regions, ECS disaster recovery provides a highly reliable disaster recovery 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 that are 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.

Features

ECS disaster recovery provides the following features:

- 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 that the business can be recovered. 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.

1.2. Service linked role for ECS disaster recovery

This topic describes the AliyunServiceRoleForHbrDr service linked role and how to delete the role.

Background information

In some cases, Hybrid Backup Recovery (HBR) 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 Service-linked roles.

The ECS disaster recovery service of HBR may need to create vSwitches, security groups, Elastic Compute Service (ECS) instances, images, and other resources. You can use the AliyunServiceRoleForHbrDr service linked role to authorize the service to access Virtual Private Cloud (VPC) and ECS resources.

Introduction

Role name: AliyunServiceRoleForHbrDr

Policy name: AliyunServiceRolePolicyForHbrDr

Policy document:

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "ecs:DescribeImages",
        "ecs: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",
```

```
        "ecs:AuthorizeSecurityGroupEgress",
        "ecs:DeleteSecurityGroup",
        "ecs:AllocatePublicIpAddress",
        "ecs:ModifyInstanceAttribute",
        "ecs:JoinSecurityGroup",
        "ecs:CreateNetworkInterface",
        "ecs:DeleteNetworkInterface",
        "ecs:DescribeNetworkInterfaces",
        "ecs:CreateNetworkInterfacePermission",
        "ecs:DescribeNetworkInterfacePermissions",
        "ecs:DeleteNetworkInterfacePermission",
        "ecs:CreateSnapshot",
        "ecs: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 in the HBR console.

For more information, see Delete a service-linked role.

1.3. Limits

This topic describes the limits of the Elastic Compute Service (ECS) disaster recovery feature on operating systems, platforms, databases, and applications.

Operating systems

The following table describes the operating systems that support ECS disaster recovery.

Operating system	Version
Windows Server	2008 R2, 2012, 2012 R2, and 2016

Operating system	Version
Linux	**Notice** You must make sure that the **/boot** partition and the **/** partition reside on the same disk. If the partitions do not reside on the same disk, move the partitions to the same disk, and then register the ECS instance for which you want to enable ECS disaster recovery. • Red Hat Enterprise Linux 7.0~7.9 • Red Hat Enterprise Linux 6.0~6.10 • CentOS 7.0~7.9 • CentOS 6.0~6.10 **Note** ECS disaster recovery is available for ECS instances that run 64-bit CentOS 6.x operating systems. If you want to implement disaster recovery for ECS instances that run 32-bit CentOS 6.x operating systems, submit a ticket. • SUSE Linux Enterprise Server 12.0~12.3 **Notice** ◦ ECS disaster recovery is available for ECS instances that run 64-bit SUSE Linux Enterprise Server 12.x operating systems. If you want to implement disaster recovery for ECS instances that run 32-bit SUSE Linux Enterprise Server 12.x operating systems, submit a ticket. ◦ If SUSE Linux Enterprise Server 12.1 runs on a VMware virtual machine, a black screen appears after you restart the virtual machine. The black screen is caused by operating system errors, but not by ECS disaster recovery. • Alibaba Cloud Linux 2.1903 LTS 64-bit The following kernel versions of Alibaba Cloud Linux 2.1903 LTS 64-bit are supported: ◦ 4.19.91-25.1.al7.x86_64 ◦ 4.19.91-24.1.al7.x86_64 ◦ 4.19.91-23.al7.x86_64 ◦ 4.19.91-22.2.al7.x86_64 **Notice** If you need to use other kernel versions, submit a ticket.

Platforms

ECS disaster recovery is implemented based on the disk-level data replication technology and is independent of the underlying platform. The following table describes the platforms that support ECS disaster recovery. If you have questions, submit a ticket.

Platform	Version
Physical machine	Full support
vSphere	5.5, 6.0, 6.5, 6.7, and 7.0

Databases and applications

You can apply the replication technology of ECS disaster recovery to all types of databases and applications.

In most cases, automated scripts are required for various applications to ensure consistency among updates. You can use the tools and scripts that are provided by Alibaba Cloud to implement ECS disaster recovery. This ensures smooth recovery of applications.

Other limits

ECS disaster recovery also has the following limits:

- If the size of a physical volume where the 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.
- Disk write limits:
  - Linux

    If the average IO size is 4 KB, the maximum disk write speed is about 10 MB/s. If the average IO size is 64 KB, the maximum disk write speed is about 30 MB/s.
  - Windows

    The maximum disk write speed is 10 MB/s.

  If the IO size is smaller or the disk write volume is larger, the Recovery Point Objective (RPO) is not affected, but the Recovery Time Objective (RTO) is prolonged.

  When you perform cross-region disaster recovery, the total throughput supported by a single site pair is 400 Mbit/s. If the data volume exceeds this limit, both the RPO and RTO may be prolonged. When you design a disaster recovery solution, you must evaluate the business situation of protected servers and estimate the amount of data written to disks.

1.4. Cross-region disaster recovery

The primary and disaster recovery systems are deployed in different regions of Alibaba Cloud. If the primary system encounters a failure, the business system switches to the disaster recovery system. Elastic Compute Service (ECS) disaster recovery provides a highly reliable disaster recovery service by deploying the primary and disaster recovery systems in different regions. 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 prevent system failures that are caused by regional disasters.

Before you begin

Before you implement cross-region disaster recovery, you must select a region to deploy the disaster recovery system. The region must be different from the region where the production environment is deployed. You must create a virtual private cloud (VPC) in the region. In addition, you must create a vSwitch for replication and a vSwitch for restoration in the VPC.

Step 1: Create a disaster recovery site pair

To create a disaster recovery site pair that provides cross-region disaster recovery protection for ECS instances in the primary site, perform the following steps:

1.
2. In the left-side navigation pane, choose **Disaster Recovery > ECS Disaster Recovery**.
3. In the upper-right corner of the **Disaster Recovery Center** page, click **+ Add**.
4. On the **Create Disaster Recovery Site Pair (Continuous Data Replication)** panel, set the parameters and click **Create**.
   i. Set Type to **Region to Region**.
   ii. Configure the primary site information.

   The primary site is used to specify the location of the server that needs disaster recovery on the cloud.

Parameter	Description
Name	Specify the name of the primary site. For example, you can specify Hangzhou Primary Site. The name can be up to 60 characters in length. The name must meet the following requirements: ■ The name cannot start with a special character or digit. ■ The name can contain only the following special characters: periods (.), underscores (_), and hyphens (-).
Region	Select the region where the primary site resides from the **Region** drop-down list. For example, you can select China (Hangzhou).
VPC	Select the VPC that is created for the primary site from the **VPC** drop-down list. For example, you can select Default VPC.

iii. Configure the secondary site information.

The compute and storage resources that are used by the secondary site are created in the specified VPC.

Parameter	Description
Name	Specify the name of the secondary site. For example, you can specify Shanghai Secondary Site. The name can be up to 60 characters in length. The name must meet the following requirements: ■ The name cannot start with a special character or digit. ■ The name can contain only the following special characters: periods (.), underscores (_), and hyphens (-).
Region	Select the region where the secondary site resides from the **Region** drop-down list. For example, you can select China (Shanghai).
VPC	Select the VPC where the secondary site resides from the **VPC** drop-down list. For example, you can select Default VPC.

Step 2: Add the ECS instances to be protected

To add the ECS instances to be protected, perform the following steps:

1. Click the **Protected Server** tab. In the upper-right corner of this tab, select the disaster recovery site pair that you created in Step 1 from the drop-down list.
2. On the Protected Server tab, click **+ Add**. Select the ECS instances and click **OK**.

   You can select 1 to 10 ECS instances.

   In the Server Status column, the status of the added ECS instances 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 enable real-time replication of ECS instances to Alibaba Cloud, perform the following steps:

1. On the **Protected Server** tab, find the ECS instance that you want to replicate and choose **More > Failover > Start Replication** in the Operation column.
2. On the **Enable Replication** panel, set the parameters and click **Start**.

Parameter	Description
Recovery Point Policy	Select the interval at which recovery points are created from the drop-down list. Unit: hours. For example, if you select 1 hour, HBR creates a recovery point every hour.
Use SSD	Specify whether to **use SSD**. If you select this check box, SSDs are used for replication. If you use SSDs, the I/O performance of the ECS instance on the cloud after server migration or failover is significantly improved. However, the usage cost increases. We recommend that you select as needed.

Parameter	Description
Replication Network	Select a replication network from the drop-down list. HBR uses this network to replicate data for disaster recovery. By default, HBR reads the available vSwitches of the secondary VPC network. If the replication network and the recovery network are not in the same zone, the RTO becomes longer. We recommend that you configure the same zone for the replication network and the **recovery network**.
Recovery Network	Select a recovery network from the drop-down list. HBR uses this network to restore data for disaster recovery. By default, HBR reads the available vSwitches of the secondary VPC network. If the replication network and the recovery network are not in the same zone, the RTO becomes longer. We recommend that you configure the same zone for the **replication network** and the recovery network.
Automatic restart after replication interruption	Specify whether to automatically resume replication if an interruption occurs.

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

i. **Enable Replicating**: ECS disaster recovery is scanning data on the ECS instance and evaluating the overall data volume. In most cases, this process takes a few minutes.

ii. **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 data volume and the network bandwidth of the ECS instance. The progress bar in the Server Status column shows the replication progress.

iii. **Replicating**: After all valid data on the ECS instance is replicated to Alibaba Cloud, Aliyun Replication Service (AReS) monitors all write operations that are performed on the disks of the ECS instance and replicates the 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 whether your applications can run as expected. A disaster recovery drill has the following features:

- Allows you to easily check whether an application can run on a restored ECS instance as expected.
- Familiarizes you with the disaster recovery process and makes sure that a smooth failover can be performed when the primary site encounters a failure.

To perform a disaster recovery drill, perform the following steps:

1. On the **Protected Server** tab, find the ECS instance and click **Test Failover** in the Operation column.
2. On the **Test Failover** panel, set the **Recovery Network**, **IP Address**, **Use ECS Specification**,

Hard Disk Type, **Recovery Point**, **Elastic Public Network IP**, and **Post Script** parameters. Then, click **Start**.

> **Note**
> - HBR automatically retains 24 recovery points that are created in the most recent 24 hours for each ECS instance.
> - If you do not select Use ECS Specification, you must set the CPU and Memory parameters.

Alibaba Cloud then runs the application on a restored ECS instance at the specified time. The disaster recovery drill does not affect real-time data replication.

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

3. Clear the drill environment.

   After the verification is completed, click **Cleanup Test 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 at the earliest opportunity to reduce costs.

Step 4: Perform a failover

Regular disaster recovery drills ensure that you can run your applications on restored ECS instances at any time. When a critical error occurs in the primary site, you can switch your workloads to the secondary site.

> **Warning** Failover is applicable to protected ECS instances where a critical error occurs. During the failover, ECS disaster recovery stops real-time data replication. To resume replication for a protected ECS instance, you must choose More > Server Operation > Restart Replication in the Operation column.

To perform a failover, perform the following steps:

1. On the **Protected Server** tab, find the ECS instance and choose **More > Failover > Failover** in the Operation column.
2. On the **Failover** panel, set the **Recovery Network**, **IP Address**, **Use ECS Specification**, **Hard Disk Type**, **Recovery Point**, **Elastic Public Network IP**, and **Post Script** parameters. Then, click **Start**.

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

3. 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 as expected 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 that are 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 a reverse replication

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

To perform a reverse replication, perform the following steps:

1. On the **Protected Server** tab, find the ECS instance and choose **More > Failback > Reversed Register** in the Operation column. In the message that appears, confirm that you want to perform a reverse registration on the ECS instance.
2. In the Actions column, choose **More > Restore > Initiate Reverse Replication**.
3. On the **Initiate Reverse Replication** panel, set the **Original machine recovery**, **Replication Network**, and **Recovery Network** parameters. Then, click **Start**.

> **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. After the ECS instance enters the Reversed Enable Replicating state, choose **More > Failback > Failback** in the Operation column.
5. On the **Failback** panel, set the **CPU**, **Memory**, **Recovery Network**, **IP Address**, and **Post Script** parameters. Then, click Start.
6. After the failback is completed, choose **More > Failover > Registration** in the Operation column to register the protected ECS instance again.

1.5. Cross-zone disaster recovery

If 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. To ensure business continuity, Elastic Compute Service (ECS) disaster recovery provides cross-zone disaster recovery for you to back up application data and switch workloads to another zone to deal with failures in a single zone at the required recovery time objective (RTO) and recovery point objective (RPO).

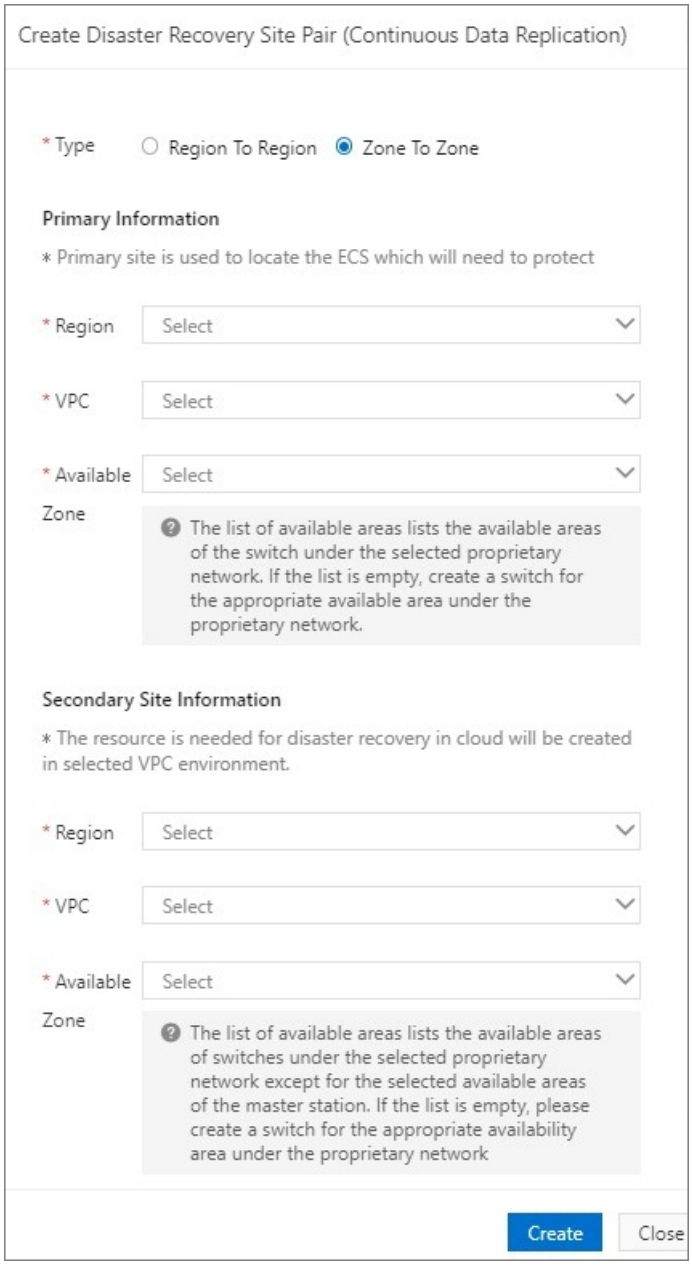
Prerequisites

A zone to deploy the disaster recovery system is selected. A virtual private cloud (VPC) is created in the zone. A vSwitch for replication and a vSwitch for restoration are created in the VPC.

Step 1: Create a disaster recovery site pair

To create a disaster recovery site pair that provides cross-zone disaster recovery protection for ECS instances in the primary site, perform the following 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. In the upper-right corner of the **Disaster Recovery Center** page, click **+ Add**.
4. In the **Create Disaster Recovery Site Pair (Continuous Data Replication)** pane, select **Zone To Zone** as Type 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, perform the following steps:

1. Click the **Protected Server** tab. In the upper-right corner of this tab, select the disaster recovery site pair that you created in Step 1 from the drop-down list.
2. On the Protected Server tab, click **+ Add**. In the Add Protected Server pane, select the ECS instances and click **OK**.

   You must select 1 to 10 ECS instances.

   In the Server Status column, verify that the status of the added ECS instances 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 enable real-time replication of ECS instances to Alibaba Cloud, perform the following steps:

1. On the **Protected Server** tab, find the ECS instance that you want to replicate and choose **More > Failover > Start Replication** in the Operation column.
2. On the **Enable Replication** panel, set the parameters and click **Start**.

Parameter	Description
Recovery Point Policy	Select the interval at which recovery points are created from the drop-down list. Unit: hours. For example, if you select 1 hour, HBR creates a recovery point every hour.
Use SSD	Specify whether to **use SSD**. If you select this check box, SSDs are used for replication. If you use SSDs, the I/O performance of the ECS instance on the cloud after server migration or failover is significantly improved. However, the usage cost increases. We recommend that you select as needed.
Replication Network	Select a replication network from the drop-down list. HBR uses this network to replicate data for disaster recovery. By default, HBR reads the available vSwitches of the secondary VPC network. If the replication network and the recovery network are not in the same zone, the RTO becomes longer. We recommend that you configure the same zone for the replication network and the **recovery network**.
Recovery Network	Select a recovery network from the drop-down list. HBR uses this network to restore data for disaster recovery. By default, HBR reads the available vSwitches of the secondary VPC network. If the replication network and the recovery network are not in the same zone, the RTO becomes longer. We recommend that you configure the same zone for the **replication network** and the recovery network.

Parameter	Description
Automatic restart after replication interruption	Specify whether to automatically resume replication if an interruption occurs.

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

i. **Enable Replicating**: ECS disaster recovery is scanning data on the ECS instance and evaluating the overall data volume. In most cases, this process takes a few minutes.

ii. **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 data volume and the network bandwidth of the ECS instance. The progress bar in the Server Status column shows the replication progress.

iii. **Replicating**: After all valid data on the ECS instance is replicated to Alibaba Cloud, Aliyun Replication Service (AReS) monitors all write operations that are performed on the disks of the ECS instance and replicates the 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 whether your applications can run as expected. A disaster recovery drill has the following features:

- Allows you to easily check whether an application can run on a restored ECS instance as expected.
- Familiarizes you with the disaster recovery process and makes sure that a smooth failover can be performed when the primary site encounters a failure.

To perform a disaster recovery drill, perform the following steps:

1. On the **Protected Server** tab, find the ECS instance and click **Test Failover** in the Operation column.
2. On the **Test Failover** panel, set the **Recovery Network**, **IP Address**, **Use ECS Specification**, **Hard Disk Type**, **Recovery Point**, **Elastic Public Network IP**, and **Post Script** parameters. Then, click **Start**.

   > **Note**
   > - HBR automatically retains 24 recovery points that are created in the most recent 24 hours for each ECS instance.
   > - If you do not select Use ECS Specification, you must set the CPU and Memory parameters.

   Alibaba Cloud then runs the application on a restored ECS instance at the specified time. The disaster recovery drill does not affect real-time data replication.

   After the disaster recovery drill is completed within a few minutes, click the link in the **Test Failover Information** column to verify restored data and applications.
3. Clear the drill environment.

After the verification is completed, click **Cleanup Test 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 at the earliest opportunity to reduce costs.

Step 4: Perform a failover

Regular disaster recovery drills ensure that you can run your applications on restored ECS instances at any time. When a critical error occurs in the primary site, you can switch your workloads to the secondary site.

> **Warning** Failover is applicable to protected ECS instances where a critical error occurs. During the failover, ECS disaster recovery stops real-time data replication. To resume replication for a protected ECS instance, you must choose More > Server Operation > Restart Replication in the Operation column.

To perform a failover, perform the following steps:

1. On the **Protected Server** tab, find the ECS instance and choose **More > Failover > Failover** in the Operation column.
2. On the **Failover** panel, set the **Recovery Network**, **IP Address**, **Use ECS Specification**, **Hard Disk Type**, **Recovery Point**, **Elastic Public Network IP**, and **Post Script** parameters. Then, click **Start**.

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

3. 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 as expected 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 that are 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 Zone A to Zone B, you can also perform reverse replication to replicate applications from Zone B to Zone A.

To perform reverse replication, perform the following steps:

1. On the **Protected Server** tab, find the ECS instance and choose **More > Failback > Reversed Register** in the Operation column. In the message that appears, confirm that you want to perform a reverse registration on the ECS instance.
2. In the Actions column, choose **More > Restore > Initiate Reverse Replication**.
3. On the **Initiate Reverse Replication** panel, set the **Original machine recovery**, **Replication Network**, and **Recovery Network** parameters. Then, click **Start**.

   > **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. After the ECS instance enters the Reversed Enable Replicating state, choose **More > Failback > Failback** in the Operation column.
5. On the **Failback** panel, set the **CPU**, **Memory**, **Recovery Network**, **IP Address**, and **Post Script** parameters. Then, click Start.
6. After the failback is completed, choose **More > Failover > Registration** in the Operation column to register the protected ECS instance again.