ALIBABA CLOUD

Alibaba Cloud

Hybrid Backup

Disaster Recovery

Document Version: 20201019

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 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

Operating system	Version
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** Disaster recovery is supported for ECS instances that run CentOS 6.x 64-bit operating systems. To implement disaster recovery for ECS instances that run CentOS 6.x 32-bit operating systems, submit a ticket. • SuSE Linux Enterprise Server 12.0~12.3 **Notice** Disaster recovery is supported for ECS instances that run SuSE Linux Enterprise Server 12.x 64-bit operating systems. To implement disaster recovery for ECS instances that run SuSE Linux Enterprise Server 12.x 32-bit operating systems, submit a ticket. If 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 Disaster recovery for ECS instances that run other Linux distributions will be supported 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. Support for more architectures are under development. For more information, submit a ticket.

Architecture	Supported 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 consistency among updates. When you implement ECS disaster recovery, you can use the available tools that are provided by Alibaba Cloud along with scripts to guarantee 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.

1.4. 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, workloads are switched 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 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.

Prerequisites

A region to deploy the disaster recovery system is selected. A virtual private cloud (VPC) is created in the region. 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-region 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 **Region To Region** 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. In the **Enable Replication** pane, set the **Recovery Point Policy**, **Use SSD**, **Replication Network**, **Recovery Network**, and **Automatic restart after replication interruption** parameters.

   > **Note** The VSwitches used for replication and restoration must be in the same zone.

   
3. Click **Start**.The ECS instance then 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. In most cases, this process takes 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 data volume and the network bandwidth of the ECS instance. 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, 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. In the **Test Failover** pane, set the **Recovery Network**, **IP Address**, **Use ECS Specification**, **Hard Disk Type**, **Recovery Point**, **Elastic Public Network IP**, and **Post Script** parameters.

> 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.

3. Click **Start**.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.
4. 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.
5. 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 failover

Regular disaster recovery drills make sure that you can run you applications on restored ECS instances at any time. When a major 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 serious 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 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. In the **Failover** pane, set the **Recovery Network**, **IP Address**, **Use ECS Specification**, **Hard Disk Type**, **Recovery Point**, **Elastic Public Network IP**, and **Post Script** parameters.

> 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 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 Region A to Region B, you can also perform reverse replication to replicate applications from Region B to Region 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 reverse registration on the ECS instance.
2. Choose **More** > **Failback** > **Initiate Reverse Replication** in the Operation column.
3. In the **Initiate Reverse Replication** pane, set the **Original machine recovery**, **Replication Network**, and **Recovery Network** parameters.

   > **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, set the **CPU**, **Memory**, **Recovery Network**, **IP Address**, and **Post Script** parameters. Then, click **Start**.
7. 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. In the **Enable Replication** pane, set the **Recovery Point Policy**, **Use SSD**, **Replication Network**, **Recovery Network**, and **Automatic restart after replication interruption** parameters.

   > **Note** The VSwitches used for replication and restoration must be in the same zone.

   
3. Click **Start**.The ECS instance then 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. In most cases, this process takes 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 data volume and the network bandwidth of the ECS instance. 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, 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. In the **Test Failover** pane, set the **Recovery Network**, **IP Address**, **Use ECS Specification**, **Hard Disk Type**, **Recovery Point**, **Elastic Public Network IP**, and **Post Script** parameters.

   > **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.

3. Click **Start**.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.
4. 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.
5. 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 failover

Regular disaster recovery drills make sure that you can run you applications on restored ECS instances at any time. When a major 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 serious 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 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. In the **Failover** pane, set the **Recovery Network**, **IP Address**, **Use ECS Specification**, **Hard Disk Type**, **Recovery Point**, **Elastic Public Network IP**, and **Post Script** parameters.

   > **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 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 reverse registration on the ECS instance.
2. Choose **More** > **Failback** > **Initiate Reverse Replication** in the Operation column.
3. In the **Initiate Reverse Replication** pane, set the **Original machine recovery**, **Replication Network**, and **Recovery Network** parameters.

   > **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, set the **CPU**, **Memory**, **Recovery Network**, **IP Address**, and **Post Script** parameters. Then, click **Start**.
7. After the failback is completed, choose **More** > **Failover** > **Registration** in the Operation column to register the protected ECS instance again.

2.VMware disaster recovery

2.1. Restore a VMware VM to an ECS instance

This topic describes how to restore a VMware virtual machine (VM) to an Elastic Compute Service (ECS) instance.

Prerequisites

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

Background information

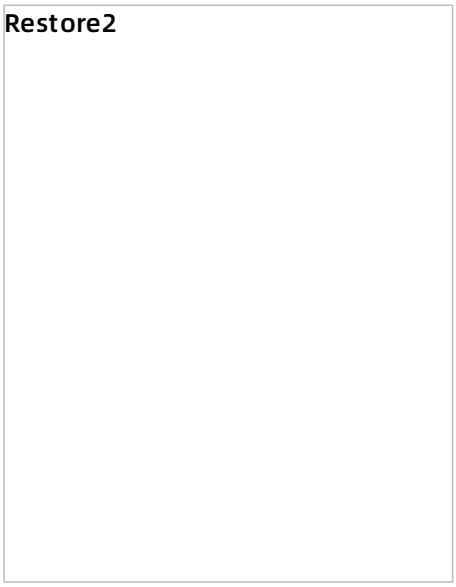
To ensure service continuity and stability of a VMware VM, you can restore the VM to an on-premises vCenter Server. However, if an infrastructure error occurs, such as an ESXi host failure or a data center failure, we recommend that you use the Hybrid Backup Recovery (HBR) console to restore the backup VM to an ECS instance.

Procedure

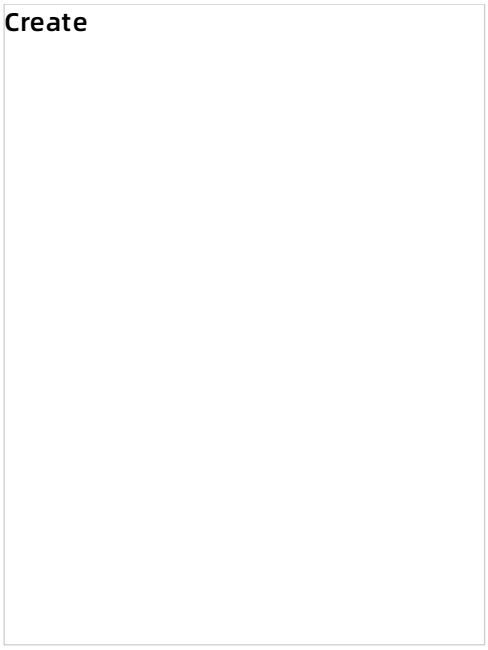
To restore a VMware VM to an ECS instance, perform the following steps:

1. Log on to the HBR console.
2. In the left-side navigation pane, choose **Disaster Recovery > VMware Disaster Recovery**.
3. On the VMware Disaster Recovery page, click the **Backup History** tab. On this tab, find the backup plan and click **Cloud Restore** in the Actions column.

4. In the Restore to ECS pane, select a VM that you want to restore, and click **Next**.



5. In the **Configure Restore Policy** step, set the **VPC**, **Switch**, **Instance Type**, **Instance Family**, and other parameters. Then, click **Create**.



6. After the restore job is created, view the restoration progress on the **Restore Jobs** tab.After the status of the restore job changes to **Mounted**, click the link in the Destination column to view the information about the ECS instance to which the VMware VM is restored.

2.2. Restore specified files on a VMware VM to an ECS instance

This topic describes how to use the instant mount feature of the Hybrid Backup Recovery (HBR) console to restore specified files on a VMware virtual machine (VM) to an Elastic Compute Service (ECS) instance.

Background information

In some scenarios, you may need to restore only specific backed-up files on a VMware VM. In this case, you can use the instant mount feature of HBR to mount the disk that stores backed-up files on the VMware VM to an ECS instance. This way, you can view and restore the backed-up files on the VM.

For more information about how to restore a VMware VM to an Alibaba Cloud ECS instance, see Restore a VMware VM to an ECS instance.

Limits

When you mount the disk of a VM to an ECS instance, note the following items:

- The ECS instance must support the file system of the disk. In addition, the file system version of the ECS instance must be the same to or later than the file system version of the disk.
- If the disk of the VM contains LVM volumes, you must ensure that LVM tools are installed on the ECS instance and the names of volume groups (VGs) and logical volumes (LVs) on the disk are different from those on the ECS instance.
- LVM volumes across disks are not supported.

- SoftRAID volumes are not supported.

Supported resources

The following OSs, volume types and file systems are supported:

- Supported OSs for the source VM: Ubuntu 20.04 LTS, Ubuntu 18.04 LTS, Ubuntu 16.04 LTS, Debian 10.X, Debian 9.X, CentOS 7.X, CentOS 8.X, RHEL 7.X, and RHEL 8.X
- Supported OSs for the destination ECS instance: CentOS 7.X and CentOS 8.X
- Supported volume types: RAW volume and LVM volume
- Supported file systems for disks: ext3, ext4, and xfs

Procedure

Perform the following steps to restore specific files on a VMware VM to an ECS instance by using the instant mount feature in the HBR console:

1. Mount a disk to an ECS instance.
   i. Log on to the HBR console.
   ii. In the left-side navigation pane, choose **Disaster Recovery > VMware Disaster Recovery**.
   iii. On the VMware Disaster Recovery page, click the **Backups** tab. Find the backup record to restore and click **Instant Mount** in the Actions column corresponding to the record.
   iv. In the **Select Disk** step, select the disk that you want to mount and click **Next**.
   v. In the **Select ECS Instance** step, select an ECS instance to which you want to mount the disk and click **Next**.

      > **Notice** Cloud Assistant must be installed on the ECS instance.

   vi. In the **Set Mount Parameters** step, confirm the settings of the **Disk Name**, **ECS Instance Name**, and **ECS Instance ID** parameters. Then, set **Mount Point** for caching and **Mount Point** and click **Create**.You can customize the path used to temporarily store the backed-up files restored from the mounted VM disk. The default path is **/tmp**. You can also customize the path to which the VM disk is mounted. The default path is **/mnt**.

      After the disk is mounted to the ECS instance, an agent is automatically installed on the ECS instance to provide access to the mounted disk.

      > **Note** The path to which the VM disk is mounted must be empty.

2. Restore files on the VMware VM.
   i. Log on to the destination ECS instance.Go to the path to which the source VM disk is mounted. View directory of each mounted volume and select the files to restore.

   ii. Run the cp command to restore the files to a specified folder.For example, you can run the **cp -v /mnt/vg3-vg3-lvdata/mnt4/govc_linux_amd64.gz /media/** command to restore the govc_linux_amd64.gz file in /mnt/vg3-vg3-lvdata/mnt4/ to the /media directory.
3. Uninstall the agent.

i. After the files are restored, ensure that the path to which the VM disk is mounted is not used.

ii. Go back to the HBR console. Click the **Restore Jobs** tab. Find the restore job and click **Uninstall** in the Actions column corresponding to the job.If the status of the job changes to **Uninstalled**, the agent is uninstalled.