ALIBABA CLOUD

阿里云

# 混合云容灾服务

# 产品简介

文档版本：20220127

阿里云

# 法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

# 通用约定

| 格式 | 说明 | 样例 |
| --- | --- | --- |
| 危险 | 该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。 | 危险<br>重置操作将丢失用户配置数据。 |
| 警告 | 该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。 | 警告<br>重启操作将导致业务中断，恢复业务时间约十分钟。 |
| 注意 | 用于警示信息、补充说明等，是用户必须了解的内容。 | 注意<br>权重设置为0，该服务器不会再接受新请求。 |
| 说明 | 用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。 | 说明<br>您也可以通过按Ctrl+A选中全部文件。 |
| > | 多级菜单递进。 | 单击**设置**> **网络**> **设置网络类型**。 |
| **粗体** | 表示按键、菜单、页面名称等UI元素。 | 在**结果确认**页面，单击**确定**。 |
| Courier字体 | 命令或代码。 | 执行 `cd /d C:/window` 命令，进入Windows系统文件夹。 |
| *斜体* | 表示参数、变量。 | `bae log list --instanceid`<br>*Instance_ID* |
| [] 或者 [a\|b] | 表示可选项，至多选择一个。 | `ipconfig [-all\|-t]` |
| {} 或者 {a\|b} | 表示必选项，至多选择一个。 | `switch {active\|stand}` |

# 目录

# 1.什么是混合云容灾服务

混合云容灾HDR（Hybrid Disaster Recovery）是一个为数据中心提供企业级应用的本地备份与云上容灾一体化的服务。可以为本地数据中心以及阿里云上面的企业关键业务提供低至秒级RPO和分钟级RTO的容灾服务，有效保障数据安全和业务连续性。

## 解决的核心问题

混合云容灾解决的核心问题如下：

- 应用级容灾保障业务持续性（Business Continuity）：在数据中心故障或长时间系统维护作业时，在云上快速恢复应用运行，缩短业务停机时间，极大减少损失。
- 数据级容灾：在数据中心备份您的数据库、虚拟机、物理机整机、备份数据存储在本地并自动上云。可在自建数据中心发生重大灾害时保障数据安全，同时提供高效的本地和云上的双重恢复。

此外，利用混合云容灾服务的服务器整机复制能力，您可以方便地将本地服务器迁移到阿里云ECS，无需重构，您就可以完成应用轻松上云。

## 支持的业务类型

**连续复制型容灾（CDR）**：为企业关键应用提供高标准容灾方案，提供秒-分级的RPO和RTO容灾。更多信息，请参见秒-分级的RPO和RTO容灾。

## 基本概念

在使用混合云容灾HDR前，您需要了解以下基本概念。

| 概念 | 描述 |
| --- | --- |
| 故障转移（Fail Over） | 即容灾恢复，指您的IDC应用出现故障时，在阿里云上恢复应用的过程。 |
| 故障恢复 （Fail Back） | 当您的IDC内的环境恢复以后，将应用数据迁回自有IDC恢复应用运行的过程。 |
| RPO | Recovery Point Objective（数据恢复点目标），指应用发生故障时预期的数据丢失量。例如，RPO = 15 分钟，表示在应用发生故障时，最近 15 分钟的数据无法在云上恢复。 |
| RTO | Recovery Time Objective（恢复时间目标），指故障发生时，在云上将应用恢复运行所需要的时间。 |
| 混合云灾备一体机 | 阿里云推出的具有容灾备份功能的一体机。 |

## 混合云容灾定价

HDR支持按量付费和包年包月资源包。关于混合云容灾HDR的计量项和计费项，请参见计费项和计费方式。

## 立即开通

立即开通混合云容灾HDR

# 2.产品优势

阿里云拥有世界水平的基础设施，随用随取的海量弹性资源，简单易用的计算、存储、网络、数据库、大数据服务，是企业天然的灾备中心。利用混合云容灾服务搭建基于阿里云的异地容灾方案是企业业务连续性和数据安全保障的理想选择。

## 总成本低廉

- 无需自建灾备中心，免去机房运维、硬件采购等成本。
- 云上主要消耗存储资源、计算资源需求极低。
- 可针对不同的应用需求以及不同的网络带宽，配置不同的 RPO、RTO，从而节约成本。
- 相对自建灾备中心的方案，可以节约高达 80% 的费用。

## 简单易用

- 云下部署简单、云上资源全自动管理、控制台集中管控。
- 备份恢复演练和容灾恢复演练可随时进行，一键启动、快速清理。

## RPO/RTO分级

企业需要对重要性级别不同的应用制定阶梯化的 RPO/RTO。企业的基础架构，尤其是网络情况会制约能达到的容灾指标。

- 连续复制型容灾（CDR）基于磁盘级实时数据复制技术，可以提供秒级-分钟级的 RPO/RTO。
- 混合云大数据容灾提供近 0 RPO 的大数据容灾，可以将 Hadoop 集群容灾至阿里云 OSS 或 EMR，在 Hadoop 集群间双向实时复制，构建大数据湖。

## 应用级容灾和数据级容灾

- 支持将 Windows、 Linux 应用服务器做高效的容灾复制和云上恢复，实现应用级容灾。
- 您可以只针对关键应用的数据，包括 SQL Server、Oracle 数据库、VMWare 虚拟机等进行定时备份和备份上云，实现数据级容灾。

# 3.应用场景

混合云容灾服务可以广泛地应用于各种数据保护和业务持续性场景。

## 关键应用的异地容灾

在本地数据中心上运行的应用可能面临各种意外情况。例如，由于软硬件环境被破坏而无法在短时间内恢复应用，火灾、自然灾害等事件甚至可能导致整个数据中心的重建。这些情况会导致关键应用长时间不可使用，从而对您的业务造成较大损失。当自有 IDC 内的应用无法短时间恢复时，混合云容灾服务能够帮助您将应用在云上快速拉起。

使用混合云容灾网关后，核心应用的服务器镜像、应用数据、文件等都被持续复制到阿里云上。如果自有 IDC 内应用出现难以恢复的故障时，您可以在阿里云上启动容灾恢复网关，快速在 ECS 上恢复应用服务器运行，使应用迅速重新上线，极大减少业务损失。平时，您还可以方便地进行容灾演练，确保真实故障发生时恢复流程顺畅，保证容灾计划的准确性。

混合云容灾服务让您无需承担自建灾备中心的巨大投入，也无需担心传统容灾方案复杂的软硬件部署运维，极大减少了异地容灾的成本，提高容灾的有效性。

## 整机云迁移

传统的上云迁移一般需要应用在云镜像上重新安装配置，ECS虚拟机重新配置，甚至应用重构等步骤，这个过程往往比较漫长。尤其是一些第三方开发的应用，因为软件依赖多且不明确、配置复杂等情况，上云迁移操作较为困难。

混合云容灾网关或者灾备一体机提供了整机备份上云并在云上恢复的方式，让您可以在 ECS 中非常方便地真实还原云下服务器环境，让上云迁移变得简单直观。

# 4.基本概念

本部分将向您介绍本产品中涉及的几个基本概念，以便于您更好地理解混合云容灾产品。

| 概念 | 描述 |
| --- | --- |
| 故障转移（Fail Over） | 即容灾恢复，指您的 IDC 应用出现故障时，在阿里云上恢复应用的过程。 |
| 故障恢复 （Fail Back) | 当您的 IDC 内的环境恢复以后，将应用数据迁回自有 IDC 恢复应用运行的过程。 |
| RPO | Recovery Point Objective（数据恢复点目标），指应用发生故障时预期的数据丢失量。例如，RPO = 15 分钟，表示在应用发生故障时，最近 15 分钟的数据无法在云上恢复。 |
| RTO | Recovery Time Objective（恢复时间目标），指故障发生时，在云上将应用恢复运行所需要的时间。 |
| 混合云灾备一体机 | 阿里云推出的具有容灾备份功能的一体机。 |

# 5.灾备规划

云容灾服务因免去了灾备中心建设、硬件系统采购、运维等复杂的工作，加上资源可弹性扩展、按量付费的特性，这些都降低了规划工作的难度。您只需花少量的时间进行选型、规划等就可以轻松使用阿里云作为您的容灾服务提供者。本文将从需求分析、RTO和RPO要求、应用的分析、灾备设备和网络环境等方面阐述如何有效地进行灾备规划。

## 需求分析

数据保护和业务连续性对数据中心的意义重大，关键应用的故障或数据丢失会对您的业务造成重大损失。混合云容灾服务提供了两个层次的能力来保护数据，并确保业务连续性。

- 异地备份
  服务器镜像和数据备份后会直接上传至阿里云灾备库，实现高可靠的云上异地备份。稳定的异地备份确保关键数据在本地数据中心发生火灾等极端情况下不丢失，在本地设施修复后恢复至本地。
- 云上容灾
  为减少因应用故障导致的业务损失，当数据中心出现严重故障无法快速恢复时，混合云容灾服务可以高效地在ECS上快速恢复您的应用。

## RTO和RPO要求

应用容灾有两个核心的指标：

- RPO：指应用发生故障时可以容忍的数据丢失量。数据越重要，RPO就要求越小。RPO越小，往往要求数据备份、复制频率更高，对生产环境、网络的压力也会越大，成本通常也越高。
- RTO：指故障发生后，期望从启动容灾恢复操作到应用恢复上线所需要的时间。故障单位时间内对业务造成的损失越大，RTO就要求越短。

RTO和RPO一般由业务部门提出要求，与IT部门共同商议，基于技术可行性、对现有系统影响、成本等多方面综合考量综合得出。RTO和RPO标准的高低与基础设施成本往往有线性关系。

您也可以参考国家和行业标准来制定RTO、RPO目标。GB/T 20988-2007标准是中国国家标准化管理委员会制定的信息系统灾难恢复规范。附录中有某行业RPO/RTO的等级规范示例，如下所示。更多信息，请参见GB/T 20988-2007标准。

| 灾难恢复能力等级 | RTO | RPO |
| --- | --- | --- |
| 1 | 2天以上 | 1天至7天 |
| 2 | 24小时以上 | 1天至7天 |
| 3 | 12小时以上 | 数小时至1天 |
| 4 | 数小时至2天 | 数小时至1天 |
| 5 | 数分钟至2天 | 0至30分钟 |
| 6 | 数分钟 | 0 |

混合云容灾服务提供了简单的配置来满足不同的RPO和RTO要求。例如，连续复制型容灾（CDR）可以提供秒级到分钟级的RPO和RTO。

## 应用的分析

容灾部署前，您需要了解关键应用的部署、环境的依赖以及应用的客户端连接等情况。

- 应用的部署
  部署关键应用前，您需要考虑以下三个要素：
  - 该应用包含哪些服务器

- 服务器之间的网络连接
- 服务器内需要做哪些配置

例如，一个简单的网页应用包含以下要素：

- 该应用包含：1个数据库服务器，1个后端服务器，1个Web前端服务器。
- 3个服务器处于同一网络。
- 后端服务器内有一个配置项指定数据库服务器IP地址，Web前端服务器有个配置项指明后端服务器IP地址。

识别这些要素之后，可以做如下计划：

- 混合云容灾服务需要保护这3台服务器。
- 阿里云上恢复时，需要将这3台服务器恢复在同一个VPC内。
- 整机恢复后，为确保这个应用能够运行，必须确保恢复时使用与云下相同的IP地址。或者，确保在恢复完成后用自动化脚本修改配置项。

- 环境的依赖
  应用容灾是一个需要多部门合作完成的过程，包括应用管理员、机房管理员和网络管理员等角色的配合实施。一个能够满足业务要求的完整的灾备方案需要考虑多个方面的细节，主要包括：
  - 应用所依赖的环境，例如Active Directory（AD）、DNS等
  - 应用所需要的网络配置

  很多情况下，应用的运行还有一些重要的环境依赖。例如在Windows环境中，很多应用都依赖AD运行。那么在云上恢复的时候，您云上的 VPC环境必须能够连接AD服务。当然，DNS服务也是很多环境下的强需求。
  以AD为例，通常会有以下两种情况：
  - 如果您已经在不同的数据中心内部署了多个主从AD服务器，那么您只需要在AD所在的数据中心和云上VPC之间能够建立高速通道或者 SSLVPN连接即可。
  - 如果您的AD服务器是集中部署在一个数据中心，可能发生同一时间离线的情况，建议您：
    - 用混合云灾备一体机保护AD服务器，在云下发生故障时首先恢复这台AD服务器。
    - 在云上VPC里部署一个从AD服务器，与云下的主AD服务器保持连接。云下发生故障时，使用云上AD。

  同样，DNS服务器也需要进行相应的配置才能满足灾备后的应用环境要求。
- 应用的客户端连接
  应用恢复后，需要确保客户端能够连接恢复出来的应用。通常情况下，您需要：
  - 如果恢复出的应用服务器IP地址与原始的一样，DNS服务器也成功恢复，那么只需要客户端与应用有网络连接即可。您可能需要用SSLVPN或者高速通道来确保客户端能与云上恢复出的应用有连接，或者恢复出的应用提供公网IP地址让客户端接入。
  - 应用恢复的时候不要求必须使用原始IP地址，您也可以修改DNS确保客户端可以连接新的服务。
  - 如果域名和IP地址都发生变化，您需要修改客户端。

## 灾备设备和网络环境

根据应用服务器的数量、数据量、RPO和RTO的标准、以及所依赖环境设施的要求，您可以合理选用灾备设备并部署合适的网络环境。

- CDR灾备一体机
  如果支持虚拟化环境，且需要容灾保护的服务器数量少于5台，建议您进行虚拟化部署。
  如果不支持虚拟化环境，或者容灾保护的服务器数量在5台以上，建议使用CDR灾备一体机。可选择的一体机型号如下所示：

| 型号 | 支持服务器数量 |
| --- | --- |
| Apsara DR100 | <20 |
| Apsara DR200 | <100 |

- 网络环境
  以上灾备设备要求的网络环境包括以下两种：
  - 数据中心到阿里云之间的网络
    - 由于优化了数据存储传输算法，混合云容灾服务并不强制要求本地数据中心与阿里云建立专线连接。但是对于大数据量、严格RPO要求的场景，建议您使用专线连接，以确保容灾服务能够达到要求的指标。
    - 应用恢复后，根据客户端、AD、DNS等与阿里云VPC的连接需求，您可能需要考虑通过SSLVPN、高速通道连接、应用暴露公网IP地址等方式来确保应用的正常使用。
  - 混合云灾备一体机到被保护服务器之间的网络
    - 为了对被保护服务器进行正常备份恢复，需要灾备一体机和被保护服务器之间有网络连接。
    - 备份一体机提供了双千兆、双万兆网卡供选择，您可以根据备份恢复吞吐要求按需配置。

# 6.HDR服务关联角色

本文为您介绍什么是混合云容灾HDR的服务关联角色（AliyunServiceRoleForHdr）以及如何删除服务关联角色。

## 背景信息

HDR服务关联角色（AliyunServiceRoleForHdr）是指在某些情况下，为了完成HDR自身的某个功能，需要获取其他云服务的访问权限，而提供的RAM角色。更多关于服务关联角色的信息请参见服务关联角色。

HDR可能需要创建新的vSwitch、安全组、ECS实例、镜像等，可通过自动创建的HDR服务关联角色（AliyunServiceRoleForHdr）获取访问VPC和ECS等资源的权限。

## AliyunServiceRoleForHdr权限说明

> **说明** RAM用户需具有HDRFullAccess权限才能创建AliyunServiceRoleForHdr。

AliyunServiceRoleForHdr具备以下云服务的访问权限：

- 云助手相关权限
  HDR需使用云助手来自动安装客户端到您的ECS实例。

```
{
      "Action": [
        "ecs:CreateCommand",
        "ecs:InvokeCommand",
        "ecs:StopInvocation",
        "ecs:DeleteCommand",
        "ecs:DescribeCommands",
        "ecs:DescribeInvocations",
        "ecs:DescribeInvocationResults",
        "ecs:DescribeCloudAssistantStatus"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
```

- ECS实例及磁盘快照相关权限
  HDR需使用ECS实例及磁盘快照相关权限来创建shadow、恢复点以及恢复实例。

```
{
      "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:ModifyResourceMeta"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
```

- 专有网络VPC的访问权限
  HDR需使用以下权限来访问您的VPC相关资源。

```
{
      "Action": [
        "vpc:DescribeVpcs",
        "vpc:DescribeVSwitches",
        "vpc:DescribeEipAddresses",
        "vpc:AssociateEipAddress"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
```

## 删除服务关联角色

如果您需要删除HDR服务关联角色（AliyunServiceRoleForHdr），您需要先删除HDR下的所有站点对。

删除服务关联角色具体操作请参见删除服务关联角色。

# 7.鉴权规则

本文提供了在混合云容灾HDR通过访问控制RAM实现团队或者部门成员鉴权、RAM用户授权、RAM角色授权、以及跨云服务授权的Action列表和Resource列表，适用于创建自定义策略实现精细化权限控制的业务需求。

## 背景信息

> **说明** 如果您无需授权就能访问目标资源，可以跳过此章节。

默认情况下，主账号或者RAM账号均能使用HDR控制台完整操作自己创建的HDR资源。在以下场景中，会涉及到操作授权问题：

- RAM账号刚创建时没有权限操作主账号的资源。
- 从其他阿里云服务访问HDR资源，或者HDR访问其他阿里云服务。
- 操作具有权限控制的HDR资源前，需要资源拥有者授权目标资源的行为权限。

当其他账号通过HDR访问主账号资源时，阿里云HDR首先向RAM发起权限检查，以确保资源拥有者已经将相关权限授予调用者。您可以阅读访问控制产品文档更多详情，实现精细化授权策略和权限控制。

## 自定义策略

您可以通过RAM控制台或者调用RAM CreatePolicy API创建一个自定义策略，在**脚本配置**方式的自定义策略中，您需要根据JSON模板文件填写**策略内容**。更多详情请参见权限策略基本元素。

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "hdr:*"
            ],
            "Resource": [
                "acs:hdr:*:15619224785*****:*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

## 鉴权列表

Action及Resource说明请参见权限策略基本元素。

| Action | Resource |
| --- | --- |
| hdr:* | acs:hdr:*:<uid>:* |

# 8.控制台概览

混合云容灾控制台是容灾服务的云上管理入口。
在混合云容灾控制台中，您可以：

- 查看容灾配置总览，包括受保护服务器的数量、类型、所有受容灾保护的数据中心数量、云上资源消耗等。
- 监控云上云下容灾网关健康状况。
- 部署云上容灾服务网关。
- 在阿里云上恢复服务器。

## 概览页面

混合云容灾控制台的概览页，如下图所示：


混合云容灾控制台的**概览**页面提供了您所使用的容灾服务的总体情况，包括：

- **容灾保护服务器数量**：您在云上和云上所有数据中心内保护的服务器数量。
- **容灾站点对数量**：自建数据中心与云上的专有网络配对的容灾站点对数量。
- **容灾存储使用量**：备份上云消耗的云上存储量。
- **容灾站点对列表**：每一个混合云容灾一体机对应一个容灾中心。该列表显示了每一个混合云灾备一体机和阿里云某个区域的配对。单击列表中的项目，您可以进入**容灾中心**页面查看详情。

## 容灾中心页面

混合云容灾控制台的容灾中心页面，如下图所示：


您可以在**容灾中心**页面中查看所有容灾中心的详情，包括：

- **站点对信息**页签：您可以查看容灾网关部署环境及所处状态、受保护服务器磁盘容量、计算平台连接状态等信息。
- **受保护服务器**页签：您可以查看该容灾中心下被保护的服务器的详细列表。
- **任务列表**页签：您可以查看容灾任务详情，如执行的任务类型、创建任务的时间等。