

# 阿里云 混合云容灾服务

## 产品简介

文档版本：20190906

# 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
	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。	 <b>禁止：</b> 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 <b>警告：</b> 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 <b>说明：</b> 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
<b>粗体</b>	表示按键、菜单、页面名称等UI元素。	单击 <b>确定</b> 。
<code>courier</code> 字体	命令。	执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。
<code>##</code>	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
<code>[ ]</code> 或者 <code>[a b]</code>	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
<code>{ }</code> 或者 <code>{a b}</code>	表示必选项，至多选择一个。	<code>swich {stand   slave}</code>

# 目录

---

法律声明.....	I
通用约定.....	I
1 什么是混合云容灾服务.....	1
2 产品优势.....	2
3 应用场景.....	3
4 基本概念.....	4
5 灾备规划.....	5
6 选型参考.....	9
7 控制台概览.....	11

# 1 什么是混合云容灾服务

---

混合云容灾服务（Hybrid Disaster Recovery，简称 HDR）是一个为您的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。

## 混合云容灾服务解决的核心问题

混合云容灾解决的两个核心问题是：

- 应用级容灾 - 业务持续性 (Business Continuity) 保障：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图云。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。

## 混合云容灾服务支持的业务类型

混合云容灾服务目前支持三种业务类型：

- 连续复制型容灾（CDR）（公测中）：解决企业关键应用的高标准容灾方案，提供秒-分级的 RPO 和 RTO 容灾。
- 快照型容灾（SDR）：解决企业核心应用的数据级容灾数据，可以对数据库、虚机、文件等实现多版本本地备份和自动备份上云。此外，还可以实现应用服务器的小时级别 RPO、RTO 的整机容灾。关于 CDR 与 SDR 的区别以及如何选择，您还可以参考[选型参考文档](#)。
- 混合云大数据容灾（公测中）：解决 Hadoop 集群数据的实时容灾复制，跨集群大数据湖建设，Hadoop 备份的问题，实现大数据集群间的近 0 RPO 实时双向复制。

## 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理想的保障选择。

### 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。
- 快照型容灾（SDR）基于数据定时备份能力，提供了小时级-天级的 RPO/RTO，并且可以与业务网络流量错峰。
- 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。

### 应用级本地与远程备份

本地备份设备的容量限制了可以保留的备份数量。备份媒介的损坏、火灾、自然灾害等情况可能导致数据的永久丢失，造成难以承受的损失。针对这些问题，远程备份成为一种主流选择，但是异地灾备中心建设的复杂性和高成本不容忽视。

混合云灾备一体机可以对服务器镜像、应用数据、文件等进行备份，并将备份数据高效保存在一体机内以备快速恢复。同时，利用重删压缩加密能力，一体机可以安全高效地将备份保存到阿里云上，提供高性能的异地备份。并且，利用云上的海量空间，您可以设置远超自有 IDC 的备份过期时间，进一步提升备份能力。

### 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。适用于快照型容灾 (SDR) 与连续复制型容灾 (CDR)。
容灾恢复网关	适用于快照型容灾，是在阿里云上按需部署的容灾恢复服务器。它可以根据云上容灾存储中的备份数据，在 ECS 上恢复您的云下服务器整机、文件和应用数据。

## 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，已经大大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。本文档将从需求分析、RTO/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三个层次的能力来保护数据，并确保业务连续性。

- 本地备份

混合云灾备一体机可以按照预设策略将服务器整机镜像和文件备份至本地，并在需要时恢复至虚拟化平台和物理平台，物理平台仅支持文件级恢复。

- 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/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 越高，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：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、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、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。

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、RTO，而快照型容灾（SDR）提供了小时级的 RPO、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，Web 前端服务器有个配置项指明后端服务器 IP。

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，必须确保恢复时用与云下相同的 IP。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，比如 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。比如在 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 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 让客户端接入。
- 应用恢复的时候不要求必须使用原始 IP，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 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、RRO/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。

· 灾备设备包括 SDR 灾备一体机和 CDR 灾备一体机：

- SDR 灾备一体机

根据需保护的服务器数量、总的的数据量、RTO/RPO 要求，您可以选择一款合适的灾备一体机。可选择的一体机型号如下所示：

型号	支持服务器数量	支持的源数据量	备份恢复吞吐
HDR1000	<20	<10 TB	0.5 TB/小时
HDR2000	20~100	20 TB~100 TB	1 TB/小时

- 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	< 50

· 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 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 选型参考

混合云容灾服务的目标是为企业的数据和应用提供稳定、可靠、易用、低成本的异地容灾能力。您可以参考快照型容灾（SDR）与连续复制型容灾（CDR）在技术指标、实现方式、应用场景上的区别，针对不同的使用场景选择相应的业务类型来保护您的关键业务和核心数据。

### 技术指标

SDR 与 CDR 在技术指标上的区别如下表所示：

指标	CDR	SDR
RPO	秒 - 分钟级	小时 - 天级
RTO	分钟级	小时级
多恢复点时限	30天	不限时长
网络要求	较高	较低
总拥有成本	较高	较低

### 应用场景

由于 SDR 与 CDR 在各项技术指标和技术实现方式的差异，您需要根据不同使用场景选择合适的容灾方案。

场景	案例	CDR	SDR
关键应用秒级 - 分钟级 RPO、RTO 容灾	企业关键业务允许 5 分钟 RPO，宕机后要求 15 分钟内在云上拉起，恢复业务运行。	√	×
重要应用小时级 RPO、RTO 云容灾	企业内重要应用需要实现 24 小时 RPO、6 小时 RTO 的应用级容灾。	×	√
关键应用数据级容灾（本地+云双备份）	本地 Oracle、SQL Server 数据库，以及一系列重要文件需要实现多版本的本地备份，同时备份数据上云，实现数据级容灾。	×	√

场景	案例	CDR	SDR
跨地域容灾	容灾系统部署在阿里云的两个地域中，当主系统发生故障时，业务系统切换到容灾系统。主系统和容灾系统部署在不同的地域，可靠性更高，有效避免了地域性灾害导致的系统故障。	√	×
跨可用区容灾	支持业务的跨可用区（Zone）容灾能力，对整体的应用做容灾备份来应对单地区的故障，满足业务的 RTO/RPO 核心指标。	√	×

总的来说，CDR 专注于为企业核心应用提供高标准 RPO、RTO 的业务持续性服务，支持 IDC 到阿里云、阿里云上跨地域和跨可用区容灾，将您因业务宕机导致的损失降到更低。

而 SDR 在纯应用数据的多版本备份能力上更具优势，为您的数据提供本地备份和云上数据容灾的双保险。同时标准型也能承载 RPO、RTO 要求不高的业务的整机容灾业务，总拥有成本也更低。

此外，CDR 与 SDR 可以混合使用来保护不同的应用，以便达到性能和成本的最佳平衡。

#### 实现方式

SDR 与 CDR 在实现方式上的区别如下：

- CDR 是基于磁盘级的数据持续复制技术来实现数据的实时上云，从而提供对关键业务的低 RPO、RTO 业务持续性保障。
- SDR 则是基于对应用和服务器整机的全自动定时备份和备份恢复来实现数据级和应用级的云容灾。

## 7 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。