

ALIBABA CLOUD

阿里云

混合云备份服务
产品简介

文档版本：20220511

 阿里云

法律声明

阿里云提醒您在使用或阅读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 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 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 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 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 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.什么是混合云备份HBR	05
2.为什么要选择混合云备份	07
3.应用场景	11
4.HBR服务关联角色	18
5.备份指标概览	25
6.使用限制	26
7.安全与合规	31
7.1. 访问控制	31
7.2. 数据加密	31
8.支持列表	32
9.开服地域	34

1.什么是混合云备份HBR

混合云备份HBR (Hybrid Backup Recovery) 作为阿里云统一灾备平台，是一种简单易用、敏捷高效、安全可靠的公共云数据管理服务，可以为阿里云ECS整机、ECS数据库、文件系统、NAS、OSS以及自建机房内的文件、数据库、虚拟机、大规模NAS等提供备份、容灾保护以及策略化归档管理。

产品架构



- 云上数据备份

阿里云ECS实例上的文件目录、自建MySQL、Oracle、SQL Server、SAP HANA、NAS、OSS等关键数据可以高效地通过内网备份到备份库，提供MySQL、Oracle数据库近0 RPO实时备份功能。其他云平台的数据也可以备份到阿里云备份库。
- 本地上云备份

将服务器本地文件、NAS文件，VMware虚拟机、数据库等数据直接备份到云备份库，备份策略设置灵活。
- 跨地域备份和ECS跨地域容灾
 - 通过镜像备份库功能实现跨地域备份，给数据提供多重保护。
 - 提供ECS秒级RPO、分钟级RTO高性能跨地域容灾。
- VMware虚拟机迁云

将本地机房VMware虚拟机无代理迁移上云，提供增量迁移方式，简单、易用、快捷。
- 本地NAS上云归档

将本地海量文件智能归档到HBR归档库，归档策略设置灵活，支持本地存储及归档库中文件内容秒级全文搜索。

基本概念

在使用混合云备份HBR前，您需要了解以下基本概念。

名称	描述
备份源	需要备份的数据所在的机器，例如服务器、虚拟机或者ECS实例。
客户端	客户端安装在备份源上。您可以通过客户端进行备份和恢复等操作。不同的备份源系统和平台需要安装相应的客户端。 客户端支持定时重试等方式确保备份稳定性，在网络短时抖动情况下依然可以完成备份。
地域	地域是指阿里云物理的数据中心。资源创建成功后不能更换地域。HBR支持的开服地域，请参见 开服地域 。

名称	描述
备份仓库	<p>备份仓库是HBR的云备份仓库，用于存储您备份在云上的数据。多个客户端可以备份到同一个仓库，帮助您更高效的管理备份数据，减小管理时间和成本。</p> <p>备份仓库支持的客户端数和存储容量没有限制，按需订阅，按需扩容，同时备份库提供12个9的数据可靠性。</p> <p>备份仓库有地域属性，选择合理的备份仓库地域可以帮助您提高备份性能，布局容灾。备份仓库创建成功后不能更换地域。数据的重删压缩都以备份仓库为单位。</p>

支持备份哪些数据源

数据源	系统	
本地数据中心	文件目录	Windows、Windows Server、Linux
	NAS	Windows、Windows Server、Linux
	VMware vSphere中的虚拟机镜像	Windows、Windows Server、Linux
	MySQL、Oracle和SQL Server数据库	Windows、Windows Server、Linux
阿里云ECS	ECS中的文件目录	Windows Server、Linux
	部署在ECS上的SAP HANA	Windows Server、Linux
	部署在ECS上的MySQL、Oracle、SQL Server	Windows Server、Linux
	云盘（系统盘、数据盘）	不涉及
云存储网关	部署在阿里云上的文件网关	不涉及
阿里云文件存储NAS	保存在阿里云文件存储NAS的数据	不涉及
阿里云对象存储OSS	保存在阿里云对象存储OSS的数据	不涉及

混合云备份定价

HBR支持按量付费和包年包月资源包。关于混合云备份HBR的计量项和计费项，请参见[混合云备份计费方式与计费项](#)。

立即开通

[立即开通混合云备份HBR](#)

2.为什么要选择混合云备份

混合云备份HBR作为阿里云统一灾备平台，提供数据备份、数据容灾保护以及策略化归档管理。

数据灾备的必要性

数据灾备是企业保护核心数据的重要手段，能有效降低勒索病毒、系统故障、自然灾害和运维事故导致的数据丢失和损坏问题，同时满足行业安全和合规要求。

- 数据面临的风险
企业数据面临勒索病毒、系统故障、自然灾害和运维事故影响，会意外导致数据丢失和损坏，其带来的影响是巨大的。
- 行业安全与合规要求
网络安全等级保护2.0、个人信息保护法、关键信息基础设施安全保护条例等各种行业规范和条例，明确规定：**维护数据的完整性、保密性和可用性**。
例如，2020年某公司核心员工私自删除数据库，直接导致公司SaaS业务崩溃，百万家商户生意停摆，公司市值蒸发超过数十亿港元。
例如，2020年，某核心工厂服务器遭到勒索病毒攻击，30TB数据被加密，要求支付2.3亿人民币的赎金。

云灾备的优势

相比传统本地机房灾备方案，云灾备方案拥有明显的优势。其在成本、上线速度、运维等方面，拥有以下优势：

对比项	混合云备份HBR方案	传统本地机房灾备方案
拥有成本	按量付费，节省TCO (Total cost of ownership)。	软、硬件采购成本高昂。
上线速度	天级部署，云服务即开即用。	需要数月、数年的建设。
运维投入	高扩展性、高可靠性、免运维。	运维复杂，人力投入大。
健壮性	异地备份一键开启，多重保护。	地域性自然灾害导致数据丢失。
演练	按需，随时，完全不影响生产。	准备时间长，代价高昂。

混合云备份HBR产品优势

- 技术优势
高效重删，精准识别重复数据。



项目	说明
功能	备份库已有的数据段无需再传，变长切片精准识别重复数据，仅上传和备份新的数据段。
优势	高效重删压缩技术，重删比可达30:1。在某些场景下使用不带重删功能的备份产品相比HBR需要30倍的备份存储空间。
价值	节约您的备份存储花费，能够在预算可控的情况下长期保留历史备份版本。同时，针对混合云场景，源端重删能力，也节省了您上云的带宽。

- 运维优势
全自动备份任务和主动监控。



项目	说明
功能	可灵活定制全量、增量（差量）、日志、实时备份策略；短信和邮件多通道告警；备份历史任务、错误日志报告控制台多方位展示。
优势	一次策略配置，全托管备份流程；端到端备份任务自动监控，出错自动告警。
价值	免运维，人力投入少，备份系统自我管理，保证数据的安全性。

- 体验优势

直观易用的控制界面。包括数据库备份计划一览表、容灾概览图、文件备份跑道式恢复点、一键启动容灾演练等。

项目	说明
功能	文件、数据库等多种备份场景、ECS容灾场景，从易用性角度为您提供具有不同特色的界面，备份、容灾按照步骤提供指导。
优势	备份计划、备份点、恢复点一目了然；让复杂的容灾操作变得容易。
价值	容易上手操作，学习成本低，运维人员更替带来的影响极小。

- 安全增强优势

为提升数据备份的安全管理水平，防止来自企业内部的意外操作或者恶意攻击，或者被未授权用户备份和恢复数据，满足安全合规要求。混合云备份HBR提供KMS加密、备份锁定、备份恢复权限分离功能。更多信息，请参见[使用安全增强特性](#)。

项目	说明
功能	<ul style="list-style-type: none"> ◦ KMS加密 ◦ 备份锁定 ◦ 备份和恢复权限分离
优势	界面化配置，KMS加密和备份锁定一键开启，配置简单。
价值	提升数据备份的安全管理水平，防止来自企业内部的意外操作或者恶意攻击，或者被未授权用户备份和恢复数据，满足安全合规要求。

综上，相比于在自建的数据中心搭建备份系统或自行搭建云上备份系统，混合云备份HBR具有以下优势：

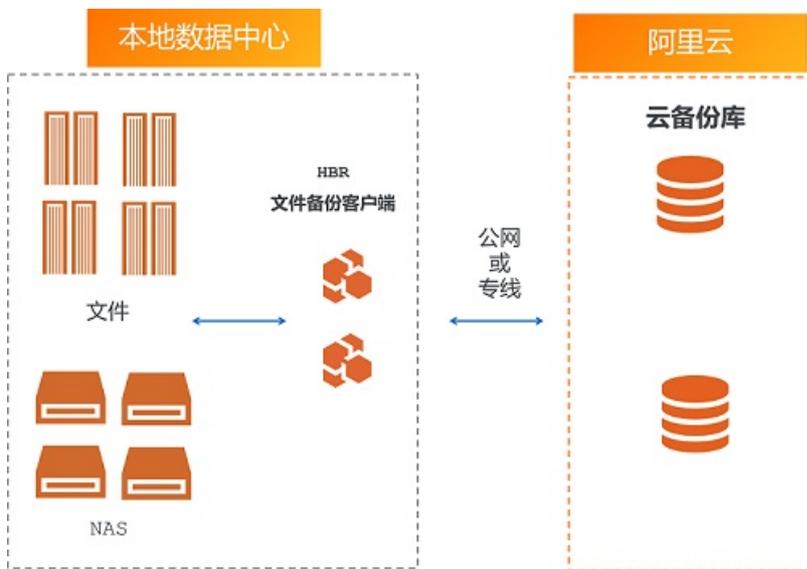
对比项	手工备份	混合云备份HBR
权限管理	无 手工备份没有严格的权限管理功能，容易出现数据误删除等操作。	有 混合云备份HBR使用RAM服务为操作人员划分等级权限，限制其访问被授权的资源。

对比项	手工备份	混合云备份HBR
重删压缩	无 重复备份的数据会增加大量的存储成本，且备份速度低。	有 混合云备份HBR采用阿里云自研的重删（重复数据删除）、压缩技术，可有效减少I/O传输量和云备份存储量，从而提高备份速度，节省成本。
备份报警	无 一旦出现备份失败，不通过人工跟踪无法感知。有些只有在恢复备份时，才发现备份失败。	有 混合云备份HBR的备份报警功能可以在备份失败或客户端与服务器连接断开时，向备份人员发送报警通知。
备份数据生命周期	手动管理	自动管理
异地备份	无	镜像仓库是备份仓库的异地镜像，镜像仓库可以帮助您实现跨地域异地备份，您还可以使用异地镜像仓库实现跨地域恢复。更多信息，请参见 跨地域备份 。
数据恢复	需手动整合多个恢复副本。	混合云备份HBR的备份版本展示清晰，方便恢复时选择，还可以设置恢复规则。
管理成本	高 手工备份需要人工写脚本、需要相应的管理人员，整体运维复杂、难度较大、资源利用率低、管理成本高。	低 使用混合云备份HBR，您只需将备份数据托管到我们的云上备份仓库，无需担心硬件预置、配置、集群扩展、安全等问题。
数据加密	需自建	全自动数据加密校验，备份数据在源端完成AES256或KMS加密后传输上云并加密保存，传输链路HTTPS二次加密，全链路数据校验。更多信息，请参见 使用安全增强特性 。
备份锁定	无	支持备份库锁定，所有备份库只能一次写入、多次读取，即WORM (write-once, read-many)。为您的备份库添加额外的保护。更多信息，请参见 使用安全增强特性 。
数据高可用性	手动管理	提供备份库多副本冗余技术，支持备份库同城冗余。更多信息，请参见 备份库（同城冗余 ZRS） 。

3.应用场景

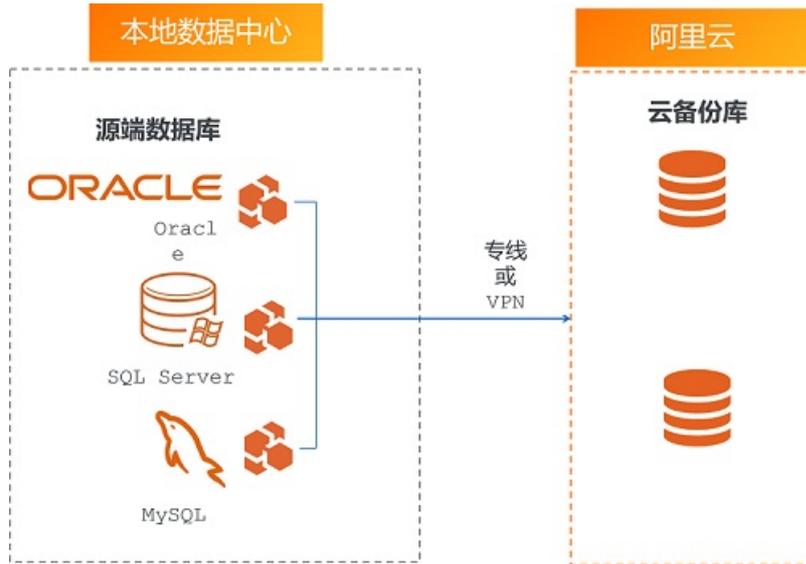
混合云备份服务HBR的典型应用场景包括：文件备份上云、数据库备份上云、大规模NAS存储Isilon极速备份上云、智能云归档、无代理VMware虚拟机迁移上云、VMware无代理备份容灾一体化、ECS备份、ECS跨AZ或地域高性能容灾和NAS、OSS无代理自动备份。

文件备份上云



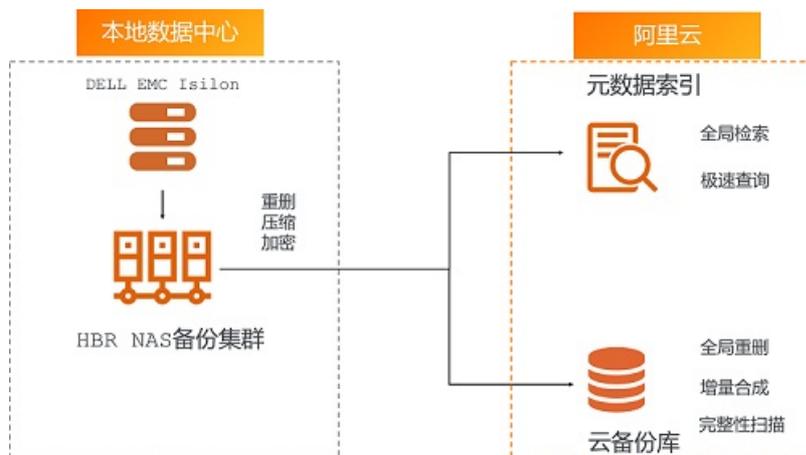
项目	说明
业务痛点	<ul style="list-style-type: none"> • 文件位置分散，备份配置难度大。 • 文件数量多，备份慢，备份SLA难以保障。 • 数据量大，本地备份硬件贵。
解决方案	<ul style="list-style-type: none"> • HBR本地文件备份，云上统一管控简化管理。 • HBR NAS备份，多节点并发提升备份速度3倍以上。 • 备份上云，本地无需硬件，重删压缩省空间和带宽。
方案价值	<ul style="list-style-type: none"> • 统一管控极大简化备份配置。 • 并发备份保障每日一备，超过预期备份SLA。 • TCO (Total cost of ownership) 费用降低了80%。

数据库备份上云



项目	说明
业务痛点	<ul style="list-style-type: none"> 数据库核心系统依赖简单脚本备份风险大。 传统一体机安装复杂，一次性投资大。 异地备份建设难。
解决方案	<ul style="list-style-type: none"> HBR备份客户端直接备份上云。 通过VPN或专线连接阿里云，进一步保障数据安全。
方案价值	<ul style="list-style-type: none"> 全面支持MySQL、SQL Server和Oracle。 无需购买一体机，安装配置简单。 直接备份上云，异地备份成本低。

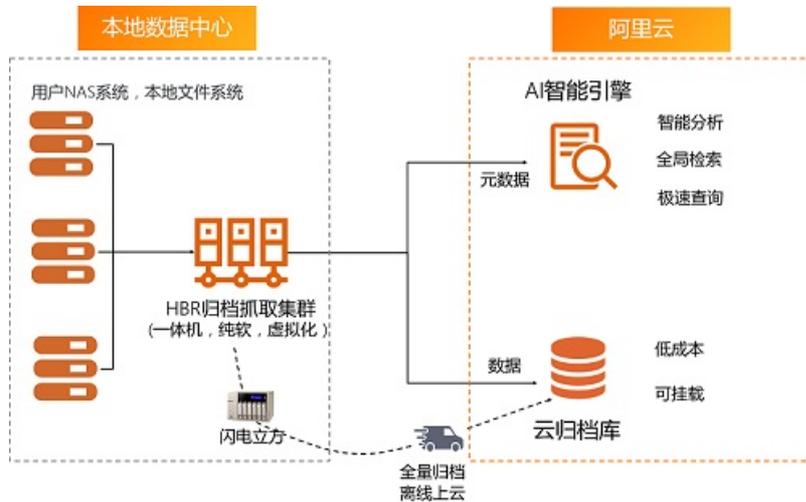
大规模NAS存储Isilon极速备份上云



项目	说明

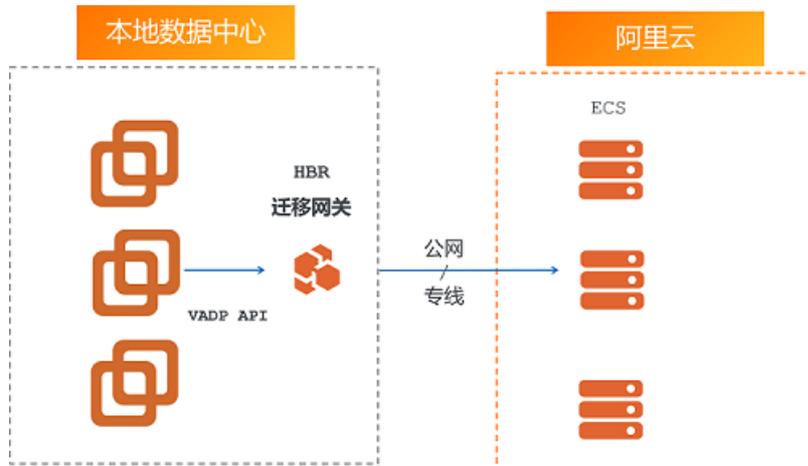
项目	说明
业务痛点	<ul style="list-style-type: none"> 文件数量多，备份慢，一次备份消耗数天到数周。 数据量大，本地备份存储硬件成本难以承受。 数据庞杂，恢复时难以快速找出对应文件。
解决方案	<ul style="list-style-type: none"> HBR对接Isilon Diff API，省去扫描周期，备份速度加快10倍以上。 多客户端并发备份，充分发挥存储与网络性能。 HBR支持全局检索，秒级搜索需恢复文件。
方案价值	<ul style="list-style-type: none"> 极大压缩备份周期，一日一备，满足您的备份需求。 全局文件搜索，提高数据管理效率5倍以上。 TCO降低70%。

智能云归档



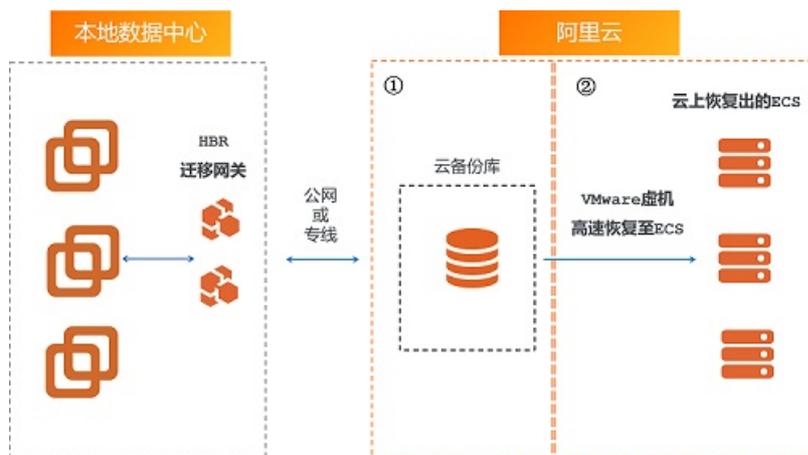
项目	说明
业务痛点	<ul style="list-style-type: none"> 归档设备建设周期漫长，成本高昂。 数据特点了解几乎为零，归档策略无法规划，归档效果无法预测。 归档数据检索困难，取回效率极低。
解决方案	<ul style="list-style-type: none"> HBR智能分析，多维度展现数据特点，针对性制定归档计划，预测归档效果。 数据存至阿里云归档库，成本极低。 HBR支持全局检索，快速发现归档文件，快速取回。
方案价值	<ul style="list-style-type: none"> 归档规划精确，策略一次配置全自动执行。 秒级搜索归档文件，快速取回。 TCO降低50%以上。

无代理VMware虚拟机迁移上云



项目	说明
业务痛点	<ul style="list-style-type: none"> 传统迁移方案对VMware有侵入性，有安全隐患，操作复杂。 数据库类虚拟机需要长时间停机才能做一致性迁移，切换时间长。 文件较多时增量迁移效率非常低。
解决方案	<ul style="list-style-type: none"> HBR无代理VMware迁移上云，无侵入性。 支持无代理增量迁移，且保障一致性。 HBR支持多虚拟机并发迁移。
方案价值	<ul style="list-style-type: none"> 无侵入无代理迁移，迁移方便。 高效增量迁移，数据库类虚拟机切换周期缩短至15分钟。

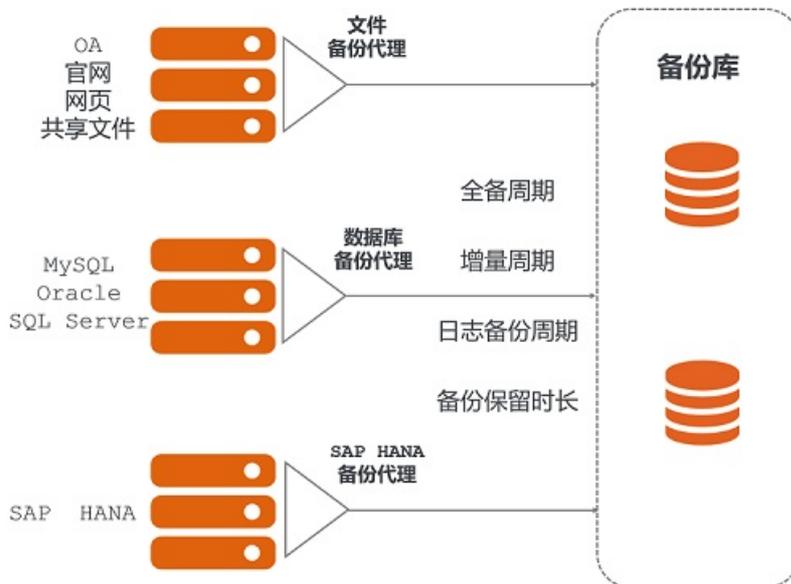
VMware无代理备份容灾一体化



项目	说明

项目	说明
业务痛点	<ul style="list-style-type: none"> 传统虚拟机备份需要备份一体机，安装配置复杂。 备份和容灾都需要独立硬件，成本高昂。
解决方案	<ul style="list-style-type: none"> HBR无代理VMware备份上云，无需本地硬件设备。 VMware备份可以云上恢复成ECS，达到容灾的目的。
方案价值	<ul style="list-style-type: none"> TCO压缩80%。 备份容灾一体化，一个方案达成两个目标。

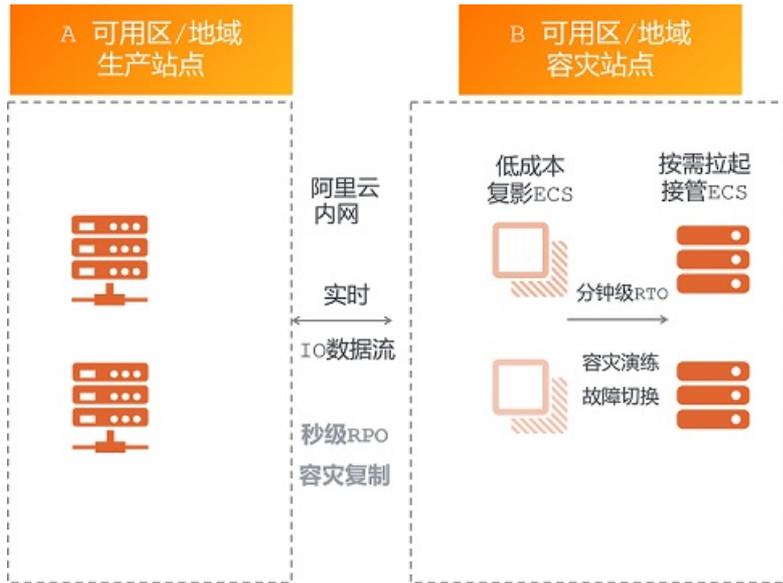
ECS备份



项目	说明
业务痛点	<ul style="list-style-type: none"> ECS数量大，备份配置管理困难。 快照无法做文件级别和数据库级别保护。 数据库备份要求高，一般备份软件难以实现。 多种数据源需求差别大，配置难，易出错。
解决方案	<ul style="list-style-type: none"> HBR ECS备份，一个服务支持ECS上所有数据类型。 数据库新老版本全面支持，提供全量、增量，日志多种备份方式。 Oracle、MySQL数据库连续日志备份，实现近0 RPO。

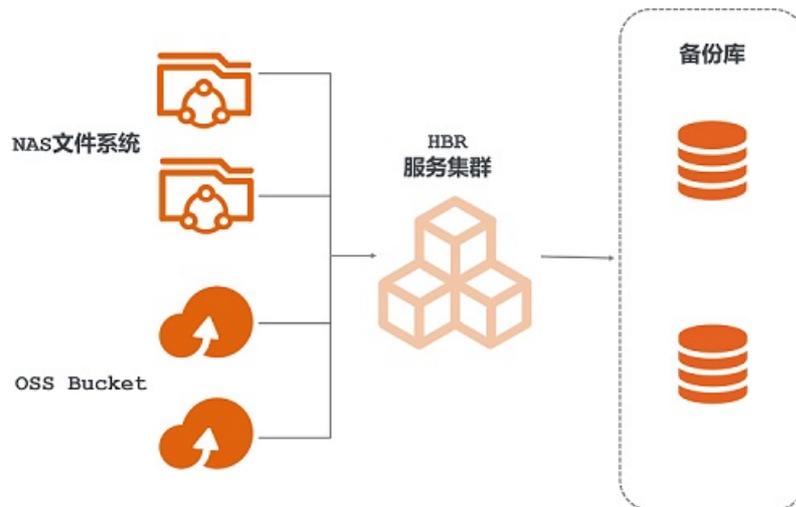
项目	说明
方案价值	<ul style="list-style-type: none"> ECS所有数据类型备份统一解决。 数据库备份高达5:1重删压缩比，文件备份高达30:1重删压缩比，数据保留一个月存储成本节约60%。 支持SAP HANA备份。获得SAP认证的公共云备份服务，备份速度可达500MB/s，恢复速度260MB/s，有效缩短RTO。

ECS跨AZ或地域高性能容灾



项目	说明
业务痛点	<ul style="list-style-type: none"> 业务容灾RPO，RTO要求高，传统方案实现难度大，成本高昂，与云平台无法做到打通。 容灾操作复杂，演练难，正确性难以保障。
解决方案	<ul style="list-style-type: none"> 基于磁盘级CDR的数据复制，可做到秒级RPO、分钟级RTO的高性能容灾方案。 HBR ECS整机跨地域容灾，无需做应用级复制，配置简单，应用一键启动。
方案价值	<ul style="list-style-type: none"> RPO < 1分钟, RTO < 15分钟。 整机容灾操作简便，随时可演练正确性，完全不影响生产环境。

NAS、OSS无代理自动备份



项目	说明
业务痛点	<ul style="list-style-type: none"> • NAS、OSS数据量大，缺乏自带定时备份机制。 • 传统方案需要在ECS上自制脚本或安装灾备软件，安装配置复杂，成本高。
解决方案	<ul style="list-style-type: none"> • HBR NAS、OSS无代理备份，无需消耗客户的ECS。 • 定时永久增量备份，确保备份效率。
方案价值	<ul style="list-style-type: none"> • 计算资源消耗为零，直接备份NAS、OSS。 • 永久增量备份和重删压缩节约存储成本可达80%。 • HBR控制台集中配置备份策略，操作简单，免运维。

4.HBR服务关联角色

本文介绍混合云备份HBR服务包含的服务关联角色，以及如何删除已创建的角色。

背景信息

HBR服务关联角色是指HBR在某些情况下，为了完成自身的某个功能，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](#)。

HBR需要访问云服务器ECS、专有网络VPC、对象存储OSS、文件存储NAS和云存储网关CSG等云服务的资源时，可通过自动创建的HBR服务关联角色获取对应的访问权限。

- `AliyunServiceRoleForHbrEcsBackup`
HBR ECS备份功能需要访问云服务器ECS和专有网络VPC云服务的资源时，可通过自动创建的HBR服务关联角色`AliyunServiceRoleForHbrEcsBackup`获取访问权限。
- `AliyunServiceRoleForHbrOssBackup`
HBR OSS备份功能需要访问对象存储OSS云服务的资源时，可通过自动创建的HBR服务关联角色`AliyunServiceRoleForHbrOssBackup`获取访问权限。
- `AliyunServiceRoleForHbrNasBackup`
HBR NAS备份功能需要访问文件存储NAS云服务的资源时，可通过自动创建的HBR服务关联角色`AliyunServiceRoleForHbrNasBackup`获取访问权限。
- `AliyunServiceRoleForHbrCsgBackup`
HBR云存储网关备份功能需要访问云存储网关CSG云服务的资源时，可通过自动创建的HBR服务关联角色`AliyunServiceRoleForHbrCsgBackup`获取访问权限。
- `AliyunServiceRoleForHbrVaultEncryption`
HBR使用KMS密钥加密备份库功能需要访问密钥管理服务KMS云服务的资源时，可通过自动创建的HBR服务关联角色`AliyunServiceRoleForHbrVaultEncryption`获取访问权限。
- `AliyunServiceRoleForHbrOtsBackup`
HBR 表格存储备份功能需要访问表格存储的资源时，可通过自动创建的HBR服务关联角色`AliyunServiceRoleForHbrOtsBackup`获取访问权限。

权限说明

HBR服务关联角色的权限内容如下：

- 通过`AliyunServiceRoleForHbrEcsBackup`获取访问ECS的权限

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

```

    "Action": [
      "ecs:AttachInstanceRamRole",
      "ecs:DetachInstanceRamRole"
    ],
    "Resource": [
      "acs:ecs:*:*:instance/*",
      "acs:ram:*:*:role/aliyunecsaccessinghbrrole"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "ram:GetRole",
      "ram:GetPolicy",
      "ram:ListPoliciesForRole"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "ram:PassRole"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Condition": {
      "StringEquals": {
        "acs:Service": [
          "ecs.aliyuncs.com"
        ]
      }
    }
  },
  {
    "Action": [
      "ecs:DescribeSecurityGroups",
      "ecs:DescribeImages",
      "ecs:CreateImage",
      "ecs>DeleteImage",
      "ecs:DescribeSnapshots",
      "ecs:CreateSnapshot",
      "ecs>DeleteSnapshot",
      "ecs:DescribeSnapshotLinks",
      "ecs:DescribeAvailableResource",
      "ecs:ModifyInstanceAttribute",
      "ecs:CreateInstance",
      "ecs>DeleteInstance",
      "ecs:AllocatePublicIpAddress",
      "ecs:CreateDisk",
      "ecs:DescribeDisks",
      "ecs:AttachDisk",
      "ecs:DetachDisk",
      "ecs>DeleteDisk",
      "ecs:ResetDisk",
      "ecs:StartInstance",

```

```

    "ecs:StopInstance",
    "ecs:ReplaceSystemDisk",
    "ecs:ModifyResourceMeta"
  ],
  "Resource": "*",
  "Effect": "Allow"
}

```

- 通过AliyunServiceRoleForHbrEcsBackup获取访问VPC的权限

```

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

```

- 通过AliyunServiceRoleForHbrOssBackup获取访问OSS的权限

```

{
  "Action": [
    "oss:ListObjects",
    "oss:HeadBucket",
    "oss:GetBucket",
    "oss:GetBucketAcl",
    "oss:GetBucketLocation",
    "oss:GetBucketInfo",
    "oss:PutObject",
    "oss:CopyObject",
    "oss:GetObject",
    "oss:AppendObject",
    "oss:GetObjectMeta",
    "oss:PutObjectACL",
    "oss:GetObjectACL",
    "oss:PutObjectTagging",
    "oss:GetObjectTagging",
    "oss:InitiateMultipartUpload",
    "oss:UploadPart",
    "oss:UploadPartCopy",
    "oss:CompleteMultipartUpload",
    "oss:AbortMultipartUpload",
    "oss:ListMultipartUploads",
    "oss:ListParts"
  ],
  "Resource": "*",
  "Effect": "Allow"
}

```

- 通过AliyunServiceRoleForHbrNasBackup获取访问NAS的权限

```
{
  "Action": [
    "nas:DescribeFileSystems",
    "nas:CreateMountTargetSpecial",
    "nas>DeleteMountTargetSpecial",
    "nas:CreateMountTarget",
    "nas>DeleteMountTarget",
    "nas:DescribeMountTargets",
    "nas:DescribeAccessGroups"
  ],
  "Resource": "*",
  "Effect": "Allow"
}
```

- 通过AliyunServiceRoleForHbrCsgBackup获取访问CSG的权限

```
{
  "Action": [
    "hcs-sgw:DescribeGateways"
  ],
  "Resource": "*",
  "Effect": "Allow"
}
```

- 通过AliyunServiceRoleForHbrVault Encryption获取访问KMS的权限

```
{
  "Statement": [
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "vaultencryption.hbr.aliyuncs.com"
        }
      }
    },
    {
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ],
  "Version": "1"
}
```

- 通过AliyunServiceRoleForHbrOtsBackup获取访问表格存储的权限

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "otsbackup.hbr.aliyuncs.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ots:ListTable",
        "ots:CreateTable",
        "ots:UpdateTable",
        "ots:DescribeTable",
        "ots:BatchWriteRow",
        "ots:CreateTunnel",
        "ots>DeleteTunnel",
        "ots:ListTunnel",
        "ots:DescribeTunnel",
        "ots:ConsumeTunnel",
        "ots:GetRange",
        "ots:ListStream",
        "ots:DescribeStream"
      ],
      "Resource": "*"
    }
  ]
}
```

删除服务关联角色

假设您已不再使用ECS备份功能，出于安全考虑，建议您删除该功能所使用的服务关联角色AliyunServiceRoleForHbrEcsBackup。

注意

- 删除AliyunServiceRoleForHbrEcsBackup、AliyunServiceRoleForHbrOssBackup、AliyunServiceRoleForHbrNasBackup和AliyunServiceRoleForHbrCsgBackup等角色前，请确保当前账号下没有备份仓库，否则删除失败。
- 删除AliyunServiceRoleForHbrVaultEncryption前，请确保当前账号下没有使用KMS加密的备份仓库，否则删除失败。

例如，删除AliyunServiceRoleForHbrEcsBackup的操作步骤如下：

1. 登录RAM控制台。
2. 在左侧导航栏中选择身份管理>角色。

3. 在角色管理页面的搜索框中，输入AliyunServiceRoleForHbrEcsBackup，自动搜索到名称为AliyunServiceRoleForHbrEcsBackup的RAM角色。
4. 在右侧操作列，单击删除。
5. 在删除RAM角色对话框，单击确定。

删除AliyunServiceRoleForHbrOssBackup、AliyunServiceRoleForHbrNasBackup和AliyunServiceRoleForHbrCsgBackup、AliyunServiceRoleForHbrVaultEncryption等服务关联角色与删除AliyunServiceRoleForHbrEcsBackup服务关联角色步骤类似，仅需替换为对应的RAM角色即可。

5. 备份指标概览

不同备份数据源支持最小备份粒度、最小备份时间间隔、备份保留时长、实时备份等功能指标是不同的。本文概要介绍各数据源支持的备份指标和备份恢复速率。

各数据源备份指标

分类	数据源	最小备份粒度	最小备份时间间隔	最长保留时间	实时备份	异地备份	账号权限隔离
本地备份上云	文件	文件	小时	永久	不支持	支持	支持
	NAS	文件	小时	永久	不支持	支持	支持
	VMware	虚拟机	小时	999年	不支持	不支持	支持
	SQL Server	库	小时 日志分钟级	永久	不支持	支持	支持
云上备份	MySQL	实例	小时	999年	支持	不支持	支持
	Oracle	表	小时	999年	支持	不支持	支持
	SQL Server	库	小时 日志分钟级	999年	不支持	不支持	支持
	SAP HANA	库	小时 日志分钟级	永久	不支持	支持	支持
	文件	文件	小时	永久	不支持	支持	支持
	NAS	文件	天	永久	不支持	支持	支持
	OSS	Prefix	天	永久	不支持	支持	支持

混合云备份HBR支持为不同账号配置不同的操作备份或者恢复权限。更多信息，请参见[创建RAM用户及授权](#)。

备份和恢复速率

混合云备份HBR的备份速率和恢复速率是在实验室测试环境下的数据，仅供您参考。更多信息，请参见[备份及恢复速率](#)。

6.使用限制

本文介绍混合云备份HBR的使用限制。

数据库备份

- 本地数据库服务器的网络必须通过专线或者VPN和阿里云专有网络（VPC）及路由（线下到云上100.64.0.0/10、100.64.0.0/11或100.96.0.0/11）互通。
- 支持的数据库版本、操作系统和备份功能有限制。更多信息，请参见[数据库备份](#)。

文件备份

- Windows客户端支持VSS快照备份。同一时间只能进行一个VSS快照备份。使用VSS时，无法备份多路径，无法备份UNC路径，无法使用通配符，无法排除文件。
- 备份时，如果文件正在被其它应用更改，但对文件有读权限，会导致备份数据不完整，需要从应用层保证要备份数据的完整性。
- 备份时，如果文件被其它进程占用或对文件没有读权限，会导致备份数据不完整，备份后状态会显示部分完成。

虚拟机备份

- 备份客户端必须使用VCenter Web Client（5.5、6.0、6.5、6.7和7.0版本）部署。
- 备份网关必须可以通过FQDN名称或者IP地址来访问管理备份虚拟机的VCenter和ESXi。
- 用于备份的虚拟机不能存在快照。在选择虚拟机阶段会提示该虚拟机已经做过快照，无法备份。若已做快照，手动删除即可。
- 无法备份有SCSI设备的虚拟机，因为VSphere VM快照不支持共享SCSI设备。
- 需要备份的虚拟机的名字不可以包含以下字符：
` ^ ~ = ; ! / () [] { } @ \$ \ & # % +`
- 以下场景无法进行增量备份（CBT模式备份）：
 - 虚拟机的硬件版本低于7。
 - 虚拟机上没有打开允许CBT模式。
 - 虚拟机磁盘模式为RDM的物理兼容模式。
 - 虚拟机磁盘模式为independent_persistent或independent_nonpersistent。

SAP HANA备份

每个环境仅支持安装一个SAP HANA实例，否则会出现“安装HANA失败”的错误提示信息。

阿里云NAS备份

阿里云NAS备份暂时不支持NAS SMB ACL特性。NAS SMB ACL特性功能详情，请参见[文件存储NAS SMB ACL特性](#)。

OSS备份

- HBR不支持备份和恢复归档存储类型的Bucket、软链接（symlink）以及Object读写权限（ACL）。
- 使用OSS清单进行备份时，为提升增量备份性能，HBR使用最近7天内最新的清单文件进行备份。生成OSS清单文件需要时间，在使用时有以下限制：
 - 备份任务触发时，如果没有任何OSS清单文件，则备份任务直接失败。
 - 备份任务触发时，如果有OSS清单文件，但是和上次相比没有更新，则备份任务失败。

- 备份任务触发时，只会使用最近一次生成的OSS清单文件进行备份。备份完成后OSS清单文件中新增文件将在下个备份周期进行备份。
- 备份执行间隔必须大于等于OSS清单的生成周期，以确保每次都能使用OSS清单文件进行备份。

ECS容灾

ECS容灾服务在操作系统、基础架构、数据库和应用等方面均有限制。更多信息，请参见[ECS容灾使用限制](#)。

VMware容灾

将VMware云上整机恢复到阿里云ECS实例前，请阅读以下阿里云ECS实例的操作系统和VMware平台的限制条件。

● Windows Server操作系统

必读项	说明
系统限制	<ul style="list-style-type: none"> ○ 请确认文件系统的完整性。 ○ 请勿修改关键系统文件。 ○ 请检查系统盘的剩余空间，确保系统盘没有被写满。 ○ 系统盘容量范围支持40 GiB~500 GiB。 ○ administrator账号的登录密码必须为8~30个字符，同时包含大小写英文字母、数字和特殊符号中的三类字符。特殊符号可以是 () ` ~ ! @ # \$ % ^ & * - _ + = { } [] : ; ' < > , . ? / 。其中，不能以正斜线 (/) 为密码首字符。
不支持项	<ul style="list-style-type: none"> ○ 不支持在系统中安装qemu-ga，否则会导致ECS所需要的部分服务不可用。 ○ 不支持以下操作系统版本： <ul style="list-style-type: none"> ■ Windows XP ■ Windows 8 ■ Windows 8.1 ■ Windows 10 ○ 不支持在Windows Server中安装社区版Virtio驱动。如已安装，请移除以下文件的只读属性。 <ul style="list-style-type: none"> ■ C:\Windows\System32\drivers\netkvm.sys ■ C:\Windows\System32\drivers\balloon.sys ■ C:\Windows\System32\drivers\vioser.sys ■ C:\Windows\System32\drivers\viostor.sys ■ C:\Windows\System32\drivers\pvpanic.sys

● Linux操作系统

必读项	说明

必读项	说明
系统限制	<ul style="list-style-type: none"> ○ 请确认文件系统的完整性。 ○ 请勿修改关键系统文件，如 <code>/sbin/</code>、<code>/bin/</code>和<code>/lib/</code>等目录。 <ul style="list-style-type: none"> ■ 请勿修改<code>/etc/issue*</code>，否则ECS无法正常识别系统发行版，从而创建系统失败。 ■ 请勿修改<code>/boot/grub/menu.lst</code>，否则无法启动ECS实例。 ■ 请勿修改<code>/etc/fstab</code>，否则无法加载异常分区从而无法启动ECS实例。 ■ 请勿将<code>/etc/shadow</code>修改为只读，否则将导致无法修改密码文件，从而创建系统失败。 ■ 不建议修改<code>/etc/selinux/config</code>文件以开启SELinux，否则系统无法启动。如果必须开启，请参见开启或关闭SELinux。 ○ 请检查系统盘的剩余空间，确保系统盘没有被写满。 ○ 开启DHCP（Dynamic Host Configuration Protocol）服务。 ○ 安装Xen或者KVM虚拟化驱动。具体操作，请参见安装virtio驱动。 ○ 安装cloud-init，以保证能成功配置hostname、NTP源和yum源。具体操作，请参见安装cloud-init。 ○ root账号的登录密码必须是8~30个字符，并且同时包含大小写字母、数字和特殊符号中的三类字符。特殊符号可以是 <code>()`~!@#\$%^&*-_+= {}[]:;<>,./?/。</code> ○ 对操作系统的GRUB版本要求： <ul style="list-style-type: none"> ■ 对于Linux系统，需要更新GRUB至1.99及以上版本。 ■ 对于CentOS 5、Red Hat 5等低版本操作系统，需要更新GRUB至1.99及以上版本。
不支持项	<ul style="list-style-type: none"> ○ 不支持多个网络接口。 ○ 不支持IPv6地址。 ○ 不支持调整系统盘分区，只支持单个根分区。 ○ 不支持在系统中安装qemu-ga，否则会导致ECS所需要的部分服务不可用。 ○ 不支持通过LVM跨磁盘构建的系统盘分区（根分区），否则可能导致ECS实例启动异常。

● VMware平台

项目	说明
vCenter版本	支持的vCenter版本包括5.5、6.0、6.5、6.7和7.0。迁移网关必须可以通过FQDN名称或者IP地址来访问管理备份虚拟机的VCenter和ESXi。

VMware虚拟机迁移

VMware虚拟机迁移服务主要针对VMware环境的虚拟机提供非侵入式的无代理整机迁移功能，其原理是基于VMware的快照以及磁盘级别的数据读取功能，将虚拟机整机全盘迁移到ECS实例上。在迁移前，请阅读以下阿里云ECS实例的操作系统和VMware平台的限制条件。

● Windows Server操作系统

必读项	说明
系统限制	<ul style="list-style-type: none"> ○ 请确认文件系统的完整性。 ○ 请勿修改关键系统文件。 ○ 请检查系统盘的剩余空间，确保系统盘没有被写满。 ○ 系统盘容量范围支持40 GiB~500 GiB。 ○ administrator账号的登录密码必须为8~30个字符，同时包含大小写英文字母、数字和特殊符号中的三类字符。特殊符号可以是 () ` ~ ! @ # \$ % ^ & * - _ + = { } [] : ; ' < > , . ? / 。其中，不能以正斜线 (/) 为密码首字符。
不支持项	<ul style="list-style-type: none"> ○ 不支持在系统中安装qemu-ga，否则会导致ECS所需要的部分服务不可用。 ○ 不支持以下操作系统版本： <ul style="list-style-type: none"> ■ Windows XP ■ Windows 8 ■ Windows 8.1 ■ Windows 10 ○ 不支持在Windows Server中安装社区版Virtio驱动。如已安装，请移除以下文件的只读属性。 <ul style="list-style-type: none"> ■ C:\Windows\System32\drivers\netkvm.sys ■ C:\Windows\System32\drivers\balloon.sys ■ C:\Windows\System32\drivers\vioser.sys ■ C:\Windows\System32\drivers\viostor.sys ■ C:\Windows\System32\drivers\pvpanic.sys

● Linux操作系统

必读项	说明

必读项	说明
系统限制	<ul style="list-style-type: none"> ○ 请确认文件系统的完整性。 ○ 请勿修改关键系统文件，如 <code>/sbin</code>、<code>/bin</code>和<code>/lib</code>*等目录。 <ul style="list-style-type: none"> ■ 请勿修改<code>/etc/issue*</code>，否则ECS无法正常识别系统发行版，从而创建系统失败。 ■ 请勿修改<code>/boot/grub/menu.lst</code>，否则无法启动ECS实例。 ■ 请勿修改<code>/etc/fstab</code>，否则无法加载异常分区从而无法启动ECS实例。 ■ 请勿将<code>/etc/shadow</code>修改为只读，否则将导致无法修改密码文件，从而创建系统失败。 ■ 不建议修改<code>/etc/selinux/config</code>文件以开启SELinux，否则系统无法启动。如果必须开启，请参见开启或关闭SELinux。 ○ 请检查系统盘的剩余空间，确保系统盘没有被写满。 ○ 开启DHCP（Dynamic Host Configuration Protocol）服务。 ○ 安装Xen或者KVM虚拟化驱动。具体操作，请参见安装virtio驱动。 ○ 安装cloud-init，以保证能成功配置hostname、NTP源和yum源。具体操作，请参见安装cloud-init。 ○ root账号的登录密码必须是8~30个字符，并且同时包含大小写字母、数字和特殊符号中的三类字符。特殊符号可以是 <code>()`~!@#\$%^&*-_+= {}[]:;<>, .?/</code>。特殊符号可以是 <code>()`~!@#\$%^&*-_+= {}[]:;<>, .?/</code>。 ○ 对操作系统的GRUB版本要求： <ul style="list-style-type: none"> ■ 对于Linux系统，需要更新GRUB至1.99及以上版本。 ■ 对于CentOS 5、Red Hat 5等低版本操作系统，需要更新GRUB至1.99及以上版本。
不支持项	<ul style="list-style-type: none"> ○ 不支持多个网络接口。 ○ 不支持IPv6地址。 ○ 不支持调整系统盘分区，只支持单个根分区。 ○ 不支持在系统中安装qemu-ga，否则会导致ECS所需要的部分服务不可用。 ○ 不支持通过LVM跨磁盘构建的系统盘分区（根分区），否则可能导致ECS实例启动异常。

● VMware平台

项目	说明
vCenter版本	支持的vCenter版本包括5.5、6.0、6.5、6.7和7.0。迁移网关必须可以通过FQDN名称或者IP地址来访问管理备份虚拟机的VCenter和ESXi。

●

7.安全与合规

7.1. 访问控制

混合云备份HBR提供基于用户的授权策略RAM Policy和STS临时授权功能，实现资源访问的控制和管理。

基于用户的授权策略RAM Policy

RAM (Resource Access Management) 是阿里云提供的资源访问控制服务，RAM Policy是基于用户的授权策略。通过设置RAM Policy，您可以集中管理您的用户（例如员工、系统或应用程序），以及控制用户可以访问您名下哪些资源的权限。

RAM Policy为JSON格式，您可以通过其中的Statement描述授权语义，每条语义包含对Action、Effect、Resource和Condition的描述。您可以根据业务场景设置多条语义，实现灵活的授权策略。更多信息，请参见[RAM简介](#)。

STS临时授权

相对于RAM提供的长效控制机制，STS (Security Token Service) 提供的是一种临时访问授权。通过STS可以返回临时的AccessKey和Token，这些信息可以直接发给临时用户用来访问混合云备份HBR。一般来说，从STS获取的权限会受到更加严格的限制，并且拥有时间限制，因此这些信息泄露之后对于系统的影响也很小。

混合云备份HBR可以通过阿里云STS进行临时授权访问。通过STS，您可以为第三方应用或子用户（即用户身份由您自己管理的用户）颁发一个自定义时效和权限的访问凭证。

7.2. 数据加密

混合云备份HBR提供备份源端加密，并支持基于SSL/TLS的HTTPS加密传输，有效防止数据在云端的潜在安全风险。

备份源端加密

混合云备份HBR支持通过密钥管理服务KMS (Key Management Service) 对数据进行加密存储，提供数据静态保护能力。KMS是阿里云提供的一款安全、易用的管理类服务。您无需花费大量成本来保护密钥的保密性、完整性和可用性。借助密钥管理服务，您可以安全、便捷的使用密钥，专注于开发加解密功能场景。您可以通过KMS控制台查看和管理KMS密钥。更多信息，请参见[密钥服务概述](#)。

基于SSL/TLS的HTTPS加密传输

混合云备份HBR支持通过HTTP或HTTPS的方式访问。安全传输层协议 (SSL/TLS) 用于在两个通信应用程序之间提供保密性和数据完整性。

8.支持列表

本文介绍混合云备份HBR支持的主流基础架构、操作系统和数据库。

基础架构

架构	支持的备份及版本
物理机	<ul style="list-style-type: none"> 文件备份：全面支持 数据库备份：MySQL、Oracle、SQL Server
虚拟机	<ul style="list-style-type: none"> 文件备份：全面支持 镜像备份：vSphere 5.5、vSphere 6.0、vSphere 6.5、vSphere 6.7、vSphere 7.0
云服务器	<ul style="list-style-type: none"> 文件备份：全面支持 SAP HANA 2.0 数据库备份：MySQL、Oracle、SQL Server

操作系统

系统	支持的版本
Windows	7、8、10
Windows Server	2008 R2、2012、2012 R2、2016、2019
RHEL	7.0、7.2、7.4、7.5、7.6、7.7、7.8、8、8.1、8.2
CentOS	6.5、6.9、7.2、7.3、7.4、7.5、7.6、7.7、7.8、7.9、8.0、8.1、8.2、8.3
Ubuntu	14.04、16.04、18.04、20.04
SUSE Linux Enterprise Server	11、12、15
Alibaba Cloud Linux	2、3

数据库

数据库	支持的版本
MySQL	4.1、5、5.0、5.1、5.4、5.5、5.6、5.7、8.0
Oracle	Oracle 9i、Oracle 10g、Oracle 11g、Oracle 12c、Oracle 18c、Oracle 19c、Oracle Data Guard 11g、Oracle Data Guard 12c
SQL Server	SQL Server 2005、SQL Server 2008、SQL Server 2008 R2、SQL Server 2012、SQL Server 2014、SQL Server 2016 (RTM)、SQL Server 2017、SQL Server 2019

更多信息，请参见[数据库备份](#)。

9. 开服地域

地域是指物理的数据中心，开服地域即支持使用混合云备份服务HBR（Hybrid Backup Recovery）产品功能的地域。本文介绍HBR支持的地域。

 **注意** 各数据源备份功能所支持的地域可能有区别，实际支持地域请以控制台为准。对于开放公测的功能，控制台会提示开放公测的地域。

HBR开服的地域、城市、Region ID的对应关系如下表所示。

地域	城市	Region ID
华北1	青岛	cn-qingdao
华北2	北京	cn-beijing
华北3	张家口	cn-zhangjiakou
华北5	呼和浩特	cn-huhehaote
华东1	杭州	cn-hangzhou
华东2	上海	cn-shanghai
华南1	深圳	cn-shenzhen
西南1	成都	cn-chengdu
中国香港	香港	cn-hongkong
亚太东南1	新加坡	ap-southeast-1
亚太东南2	悉尼	ap-southeast-2
亚太东南3	吉隆坡	ap-southeast-3
亚太东南5	雅加达	ap-southeast-5
亚太东南6	马尼拉	ap-southeast-6
亚太南部1	孟买	ap-south-1
亚太东北1	东京	ap-northeast-1
美国西部1	硅谷	us-west-1
美国东部1	弗吉尼亚	us-east-1
欧洲中部1	法兰克福	eu-central-1
中东东部1	迪拜	me-east-1

使用HBR的本地服务器备份、ECS文件备份、数据库备份功能时，需要在备份对象安装HBR备份客户端。备份客户端用于和HBR服务端进行消息传递和通信控制。如果您想了解备份客户端使用的域名和端口清单，请参见[HBR客户端访问服务接入点和端口都有哪些](#)。