vinchin
云 祺 科 技

云祺容灾备份系统

技术白皮书

产品版本 V6.0

成 都 云 祺 科 技 有 限 公 司

Chengdu Vinchin Technology Co.,Ltd.

关于云祺

成都云祺科技有限公司是中国专业的云端数据保护整体解决方案提供商。为用户提供云环境及传统环境下的数据迁移、备份、恢复、容灾演练等整体解决方案。云祺科技核心团队拥有多年的数据保护产品研发经验，经过长期的技术积累，针对云环境的特点，推出新一代云祺容灾备份系统，提供对云基础设施、云架构平台以及深入到应用的全方位智能数据保护。云祺容灾备份系统是云祺科技经过深入技术研究开发的，不仅满足传统信息化业务环境数据备份要求，同时无缝支持云环境的新一代数据保护系统。并且满足公有云、私有云、混合云，应对各种复杂业务环境，软件弹性架构设计，提供对虚拟机的备份/恢复。

版权所有

使用声明

本文档仅提供阶段性信息，由于产品版本升级或其它原因，所含内容根据产品的实际情况随时更新，恕不另行通知。如因文档使用不当造成的直接或间接损失，本公司不承担任何责任。

前言

文档说明

感谢您选用云祺备份产品，本文档主要介绍云祺容灾备份系统各个模块的技术原理说明，皆在协助工程师了解云祺容灾备份系统各个功能模块备份的技术原理。

适用对象

本文档建议适用于以下对象：

- 售前工程师
- 技术工程师
- 实施工程师

目录

1. 产品概述

1.1. 产品介绍

云祺容灾备份系统（Vinchin Disaster Recovery）是由成都云祺科技有限公司完全独立自主研发的云环境和传统环境下的数据保护产品，操作简单，安全可靠，满足多种场景下的备份需求。为用户提供在私有云、公有云、混合云环境下的虚拟机备份与恢复、数据库实时与定时备份、异地副本、文件备份、数据归档、灾难恢复演练等解决方案，解决由于人为误操作、病毒攻击、逻辑错误、硬件故障和自然灾害等原因造成的数据丢失，为用户业务系统提供安全保障。

云祺容灾备份系统采用图形化的WEB管理界面，可在任意设备上（PC/手机/平板电脑）对用户数据中心的备份/恢复任务进行管控。为用户提供每日、每月、每周、一次性、滚动等备份策略，结合短信、邮件告警通知等功能，可实现真正意义上的备份系统无人值守，用户只需进行首次任务配置，即可进行全自动备份。同时，云祺容灾备份系统拥有国内首创的虚拟机瞬时恢复技术，当用户数据中心发生灾难或故障时，用户只需通过恢复任意备份时间点，即可将数据中心恢复至灾难发生前的生产状态，为用户业务连续性提供安全保障。云祺容灾备份系统满足虚拟机、数据库、文件、操作系统，异地容灾、云归档等多种备份场景，可应用至政府、军队、医院、学校、研究所、设计院、军工、大型企业、国有企业等用户，是一款简单、快速、高效的数据保护产品。

1.2. 产品架构

1.2.1. 名词解释

1. 快照技术

快照是指定数据集合的一个完全可用拷贝，该拷贝包括相应数据在某个时间点的映像。快照可以是其所表示数据的一个副本，也可以是数据的一个复制品。快照可用于在线数据备份与恢复。目前实现快照的主流技术包括：

写时拷贝（Copy On Write）：执行快照操作后，数据第一次写入到某个存储位置时，首先将原数据读出来，写到另外为快照保留的存储空间，然后再将数据写入到存储设备中。而下次针对这一位置的写操作将不再执行写时复制操作。

写时重定向（Redirect On Write）：执行快照操作后，写操作会进行重定向，所有的写操作都被重定向到新卷中，所有旧数据均保留在只读的源卷中。因此，每次生成的快照文件都是放在连续的存储区域中，同时解决了COW写两次的性能问题。因其存储性能较好，目前虚拟化平台主要采用写时重定向快照技术。

2. 虚拟机CBT

数据块修改跟踪技术(Changed Block Tracking)是虚拟化平台简化和提高虚拟机备份效率的重要组成部分，它可以实现只备份变化块数据，而不需要备份全部数据，从而减少备份数据，提高备份效率。

3. 完全备份

完全备份是对目标数据，比如虚拟机、磁盘、逻辑磁盘、文件系统等所有数据进行完全拷贝。这种备份方式的特点是数据最全面、最完整，数据一致性得到完全保护。当发生灾难时，只要用最新完全备份点，就可以恢复全部数据。

由于完全备份的数据量非常大，占用备份存储空间较多，因此，备份时间较长。而且，如果两次完全备份操作间隔较短，则存在大量的重复数据，实际上只有一小部分数据发生了变化，因此完全备份频率一般较低。

4. 增量备份

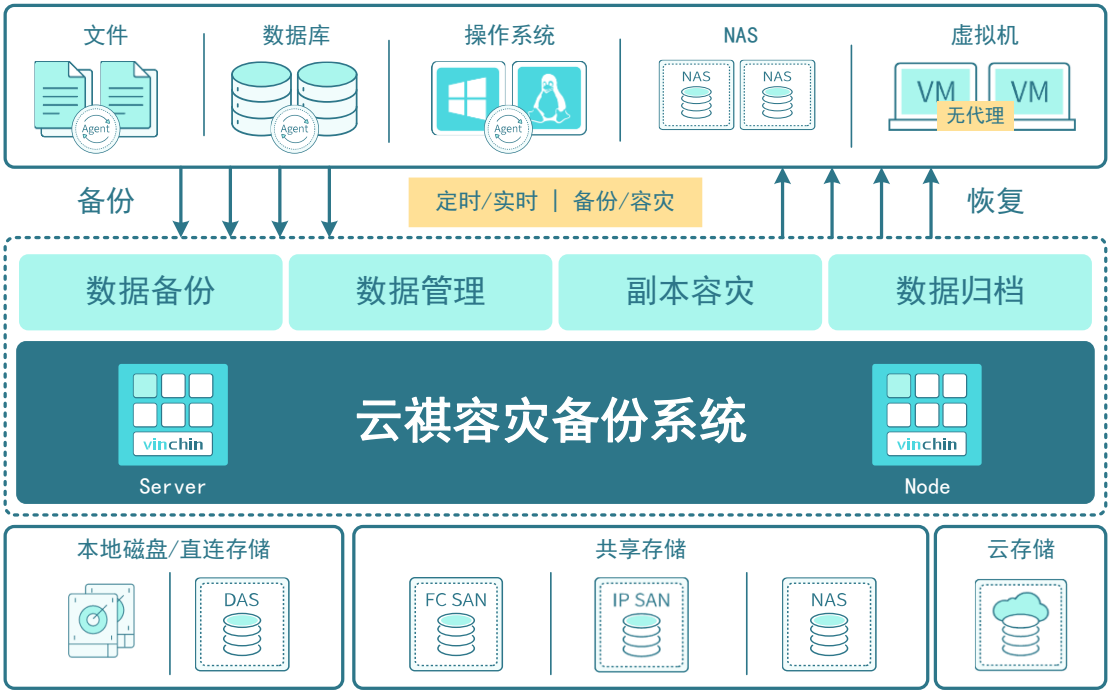
增量备份只拷贝上次备份以来发生的数据变化。在大多数情况下，连续两次备份之间只有小部分虚拟机数据发生变化。增量备份可以利用此特性，减少备份资源需求，提高备份效率，增加备份频率。

5. 差异备份

差异备份每次备份的数据是在上一次完全备份之后变化的数据，依赖上一个完全备份点

进行差异备份。差异备份较完备时间间隔越长，变化数据越多，备份数据越大，差异备份点之间没有依赖关系。

1.2.2. 技术架构



云祺容灾备份系统可对虚拟化环境和传统物理机应用环境进行数据备份与恢复。

- 虚拟机备份采用无代理方式，不需要在虚拟机内部安装备份代理。
- 虚拟机 LAN-Free 备份使用基于 SAN 的存储网络，直接从 SAN 存储设备传输数据，提高备份速度，并减少对网络的负载。
- 传统物理机备份需要在应用所在操作系统安装备份代理。

1.2.3. 系统组件

主控节点（Server）：云祺容灾备份系统管理节点，具有WEB管理和备份功能；

备份节点（Node）：由Server统一管理控制，一个Server可以管理多个备份节点；

传输代理（Proxy）：VMware 及OpenStack平台部署备份传输代理虚拟机，代理传输数据；

备份代理（Agent）：传统有代理备份，在应用服务器操作系统内部安装代理传输数据。

2. 功能模块

2.1. 主机保护

云祺容灾备份系统支持通过在WEB页面上对海量的桌面、文件服务器、数据库服务器进行批量在线代理推送安装和管理，解决了传统手工安装的高工作量和高复杂度问题。同时云祺主机保护代理支持两种连接模式以适应跨站点，公有云等多种部署场景。

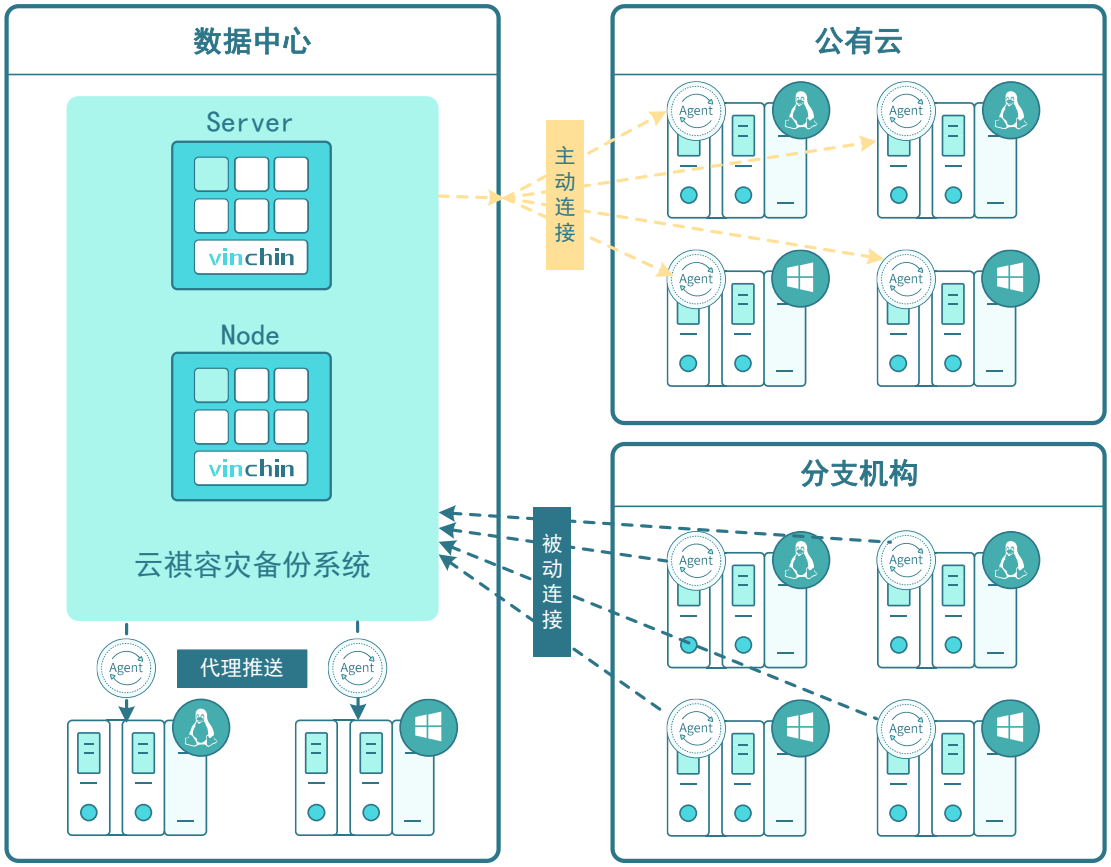


图 2-1 主机保护代理管理

云祺容灾备份系统主机保护代理管理特点：

- **All-In-One**：文件、数据库、操作系统及实时保护功能集成在同一个代理程序安装包中，便于管理及部署；
- **批量代理推送部署及管理功能**：用户可通过备份系统 WEB 页面，配置向同一网络环境中的 Windows/Linux 主机批量推送并自动安装主机保护代理程序；
- **主动/被动两种连接模式**：云祺提供主动和被动两种客户端模式，主动连接意为需保护主机安装客户端后会主动连接至云祺容灾备份系统，在管理界面即可显示该客户端，适用于被保护的主机与云祺容灾备份系统处于同一网络环境中，而被动连接则需要客户端开放指定的端口，云祺容灾备份系统通过指定的端口去连接此客户端，适用于被保护的主机无法访问到云祺容灾备份系统，而云祺容灾备份系统能连接被保护的主机。

2.1.1. 文件保护

文件保护模块应用于拥有海量非结构化数据的服务器、海量桌面备份场景，图 2-2为文件保护模块技术原理图。

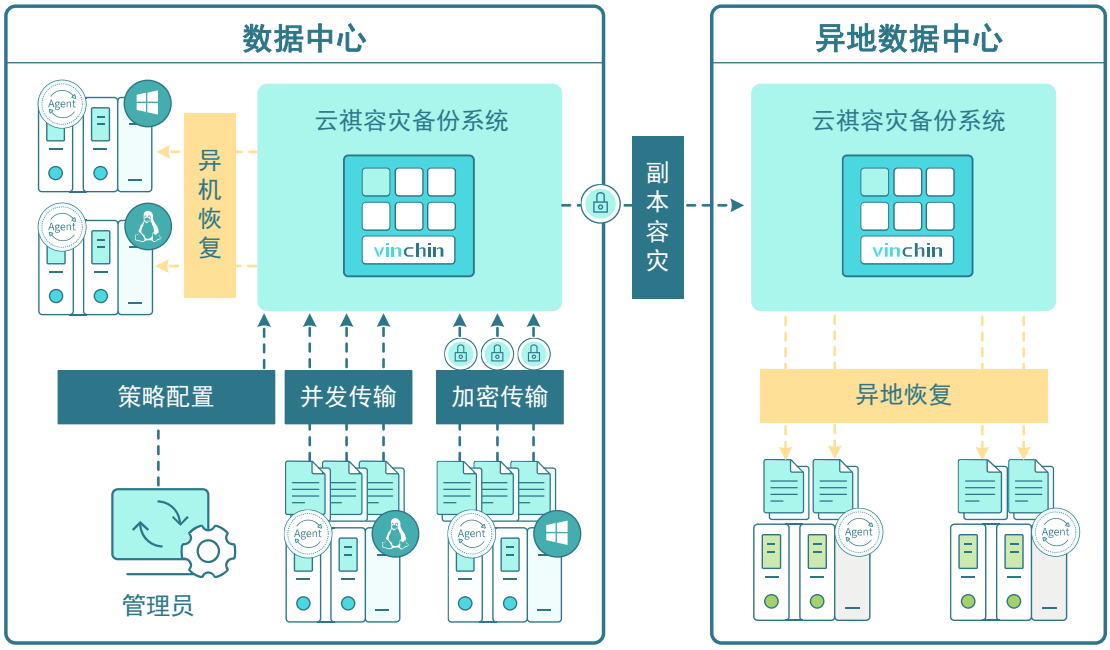


图 2-2 文件备份流程图

文件保护模块主要特点如下：

- **备份类型**：支持完全备份、增量备份、差异备份；
- **备份粒度**：目录和文件；
- **数据保留策略**：支持按照天数和按照个数保留备份数据；
- **压缩存储**：支持备份数据压缩存储；

- **小文件备份加速**：文件备份模块支持通过边扫描边传输，小文件合并打包传输等方式减少网络交互，提高备份效率；
- **多个客户端批量应用备份任务配置**：对于具有共性的海量桌面文件备份需求，云祺容灾备份系统提供了对 1 个主机配置任务后将任务批量应用于海量主机之上，大幅降低用户配置任务所需时间；
- **排除匹配备份、指定匹配备份**：支持精确匹配和模糊匹配的排除/指定文件或子目录的备份功能；
- **灵活的任务并发配置**：文件保护模块提供两级并发配置，第一级为任务的并发，可对单主机配置多个备份/恢复任务；第二级支持在单个任务中配置并发传输的通道数量，以确保在带宽充足的情况下达到最优备份/恢复效率；
- **恢复粒度**：最小恢复单位为单个文件；
- **恢复方式**：支持原机、异机备份恢复，支持同构系统或者异构系统备份数据恢复，支持覆盖恢复和新建恢复；
- **限速功能**：支持对单个任务的多种限速配置策略，提供单任务按时按需限速策略，如：工作日中 8：00-18：00 之间限速在 50M/s，18：00-20：00 限速在 100M/s，其他时间不限速的组合限速策略；
- **可配置备份网络**：可在任务配置过程中，指定每台主机的备份/恢复网络，以获取最佳数据传输效率；
- **安全保障**：支持基于 AES256 的加密传输和数据加密存储，从网络到存储层面保证数据的安全性；

2.1.2. 数据库保护

数据库管理系统（DBMS）作为目前大量应用软件、核心系统的数据存储和管理软件内部存储的数据，已经成为许多企业赖以生存的命脉，并且随着IT环境的日益复杂，越来越多用户环境同时存在多种不同的数据库管理系统。在如此复杂的情况下，如何可靠、高效的保护数据库中的数据，成为不可忽视的问题。

云祺容灾备份系统数据库保护模块能够兼容目前国内外大部分主流的数据库，支持 Oracle、SQL Server、MySQL、MariaDB、PostgreSQL、达梦、人大金仓、优炫、瀚高等数据库。采用可视化的配置向导，通过简单几个步骤即可完成对数据库的备份任务配置，结合短信/邮件告警等功能，基本保证备份系统无人值守，能够有效解决传统方案中管理员采用手工编写脚本进行备份所存在的管理难，门槛高，恢复成功率低等问题。

数据库保护模块技术原理图如图 2-3所示。

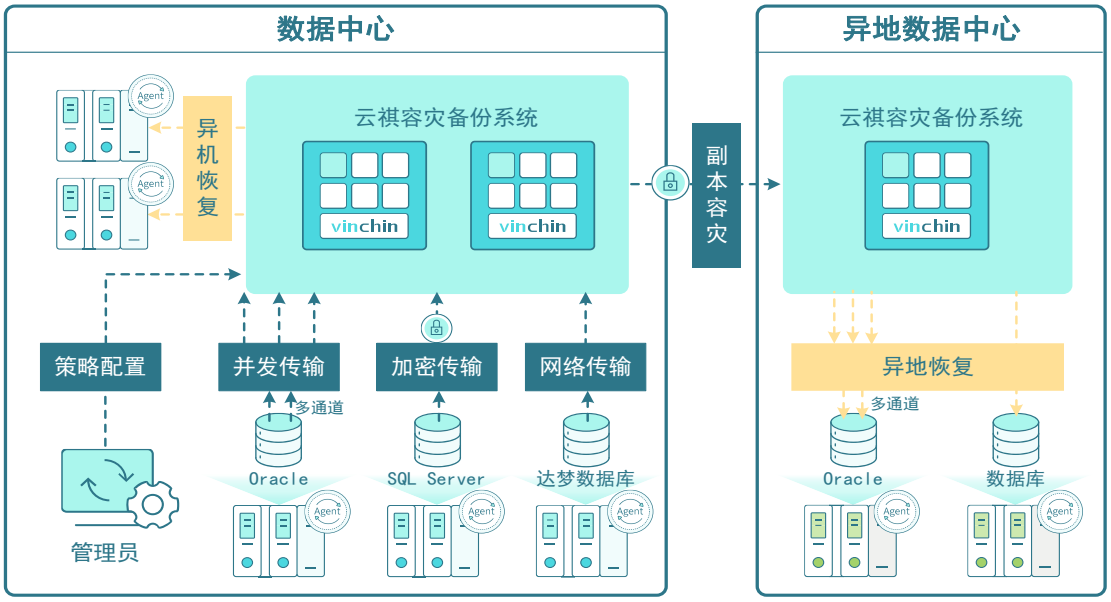


图 2-3 数据库保护技术原理图

数据库保护模块主要特点如下：

- 备份类型：
  - Oracle、DM：支持完全备份、增量备份、差异备份、日志备份；
  - SQL Server：支持完全备份、差异备份、日志备份；
  - MySQL、MariaDB：支持完全备份、增量备份、日志备份；
  - KingBase、PostgreSQL、UXDB、HighGo DB：支持完全备份、日志备份；
- 备份粒度：
  - Oracle、DM、MySQL、MariaDB、PostgreSQL、KingBase、UXDB、HighGo DB：支持实例备份；
  - SQL Server：支持数据库备份；
- 日志备份数据恢复方式：针对通过日志备份而产生的备份数据，能够恢复到两次备份之间的任意时间点；
- 备份过程不占用生产存储空间：部分解决方案采用的是先通过导出数据库备份数据，临时存储在生产空间上，之后通过代理将导出的数据库备份文件传输到备份服务器之上的方案，该方案存在对生产环境造成较大负载、效率低下、失败率高等问题；云祺容灾备份系统的数据库保护模块采用流式备份方案，是直接将备份数据通过块级方式由内存直接发送到网络，传输到备份服务器之上，解决部分方案所带来的问题；
- 灵活的网络配置项：支持配置多线程传输、加密传输、指定传输网络；
- 多种节省备份存储空间的手段：支持备份数据源端高级压缩（SQL Server/Oracle/DM）、备份数据压缩、备份数据重复数据删除等功能；
- 恢复方式：支持覆盖恢复、新建恢复、指定目录恢复以及异机恢复；

- 支持数据库多种部署模式的备份：支持 Oracle RAC 和单机环境的备份；支持 SQL Server 故障转移集群和单机模式；
- 提高 Oracle 备份效率：数据库保护模块可以通过配置 BCT（Block Change Tracking）、Oracle 备份/恢复时的通道数提高任务执行效率；
- 归档日志自动删除（Oracle/DM/Kingbase/HighGO DB/UXDB/PostgreSQL）：支持备份完成后自动删除归档日志，避免归档日志过大占用生产存储空间；
- 归档存储空间告警（Kingbase/HighGO DB/UXDB/PostgreSQL）：可按照剩余归档存储空间百分比配置告警，备份任务启动时，一但生产端归档存储空间低于配置阈值，任务会自动报错，结合短信/邮件告警功能，能够第一时间告知用户空间不足的情况，避免因空间不足执行备份任务造成生产端异常。
- MySQL 和 MariaDB 高级特性：在使用 InnoDB 作为引擎时，备份无需进行锁表操作；

2.1.3. 操作系统保护

操作系统保护模块提供对用户环境中的服务器、主机进行磁盘数据块的备份功能，采用块备份的技术手段，在用户生产主机发生软硬件故障的情况时，通过定制的LiveCD引导后，可通过备份系统，将备份数据恢复到原主机或新主机上。

操作系统保护模块流程图如图 2-4所示。

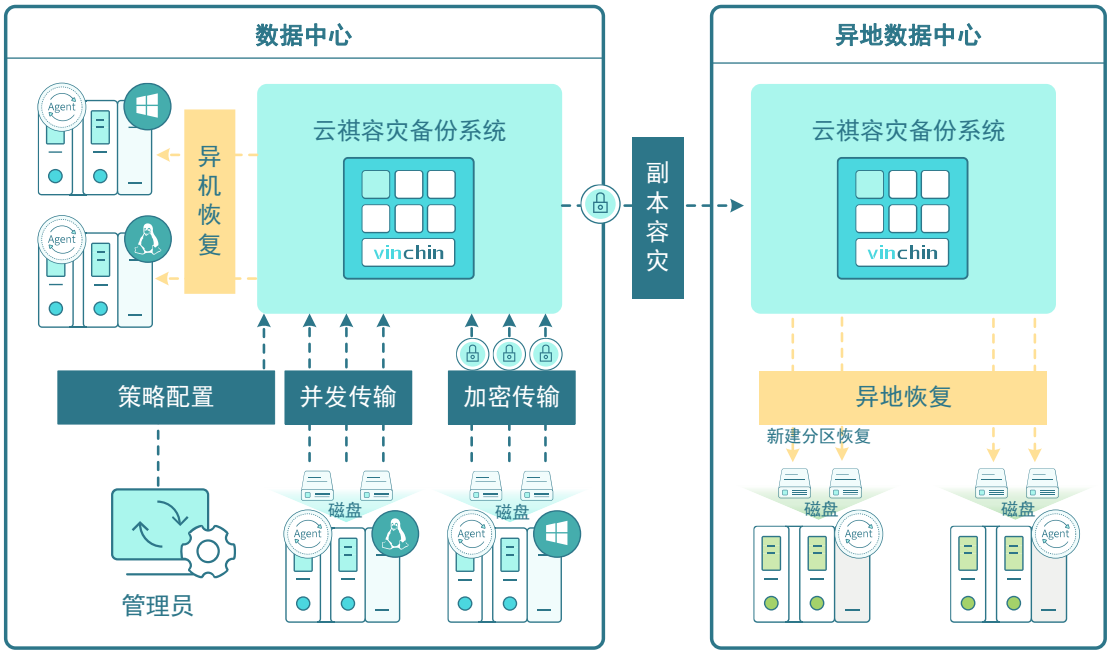


图 2-4 操作系统保护模块技术原理图

操作系统保护模块主要特点如下：

- **备份类型**：支持完全备份、增量备份、差异备份；
- **灵活的整机备份方案**：单个备份任务可配置多台需要保护的主机，同时用户可根据需求勾选单个主机下的磁盘、分区或卷；
- **数据保留策略**：支持按照天数和按照个数保留备份数据；
- **压缩及重删存储备份数据**：支持备份数据压缩存储，块级的重复数据删除；
- **主机数据一致性保证**：Windows 主机可通过 Windows VSS 在备份阶段保证数据一致性。 Linux 主机由于并未集成类似 Windows VSS 的相关框架和工具，系统无法通过自身提供的工具在备份阶段保证数据一致性；为解决该问题，主机保护代理程序中包含了由云祺自主研发的 Linux 快照功能，能够通过创建快照保证 Linux 主机的数据一致性。
- **恢复粒度**：最小恢复单位为单个分区；
- **灵活的恢复对象配对**：支持灵活的恢复分区配置，支持按源分区结构恢复到目标磁盘，同时支持将来自不同磁盘的分区恢复到一个容量更大的磁盘之中，以适用于多样的恢复需求和场景；
- **限速功能**：支持对单个任务的多种限速配置策略，提供单任务按时按需限速策略；

• **安全保障**：支持基于 AES256 的加密传输和数据加密存储，从网络到存储层面保证数据的安全性；

2.1.4. 实时容灾保护

通过结合卷远程复制技术和持续数据保护技术、以及高可用技术的原理，针对RTO和RPO敏感度较高的用户云祺科技推出了实时容灾保护模块。该模块支持实时备份和容灾接管两种模式。

实时备份模式：只需要在用户环境中部署一套云祺容灾备份系统并在用户主机上安装主机保护代理即可实现，实时备份任务启动后，在首次同步之后就会进入实时备份阶段，一但生产主机发生故障，用户可通过恢复向导将实时备份任意时间点环境恢复到原主机或者新主机上。原理如图 2-5 所示。该模式RPO≈0，RTO为恢复数据大小除恢复链路带宽，适用于对RTO要求不高，但是需要在故障发生后尽量少丢失数据的用户。

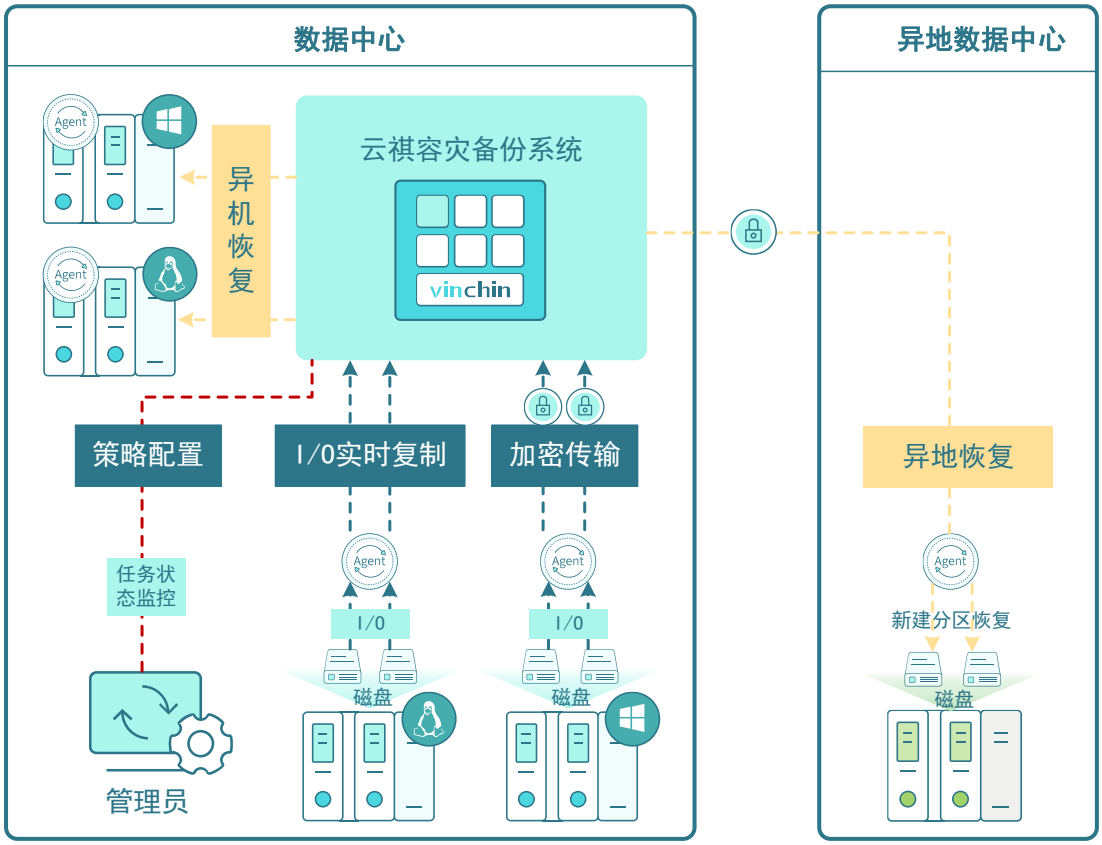


图 2-5 实时备份部署模式

容灾接管模式：该模式在实时备份部署模式的基础上还需要配置额外的备用主机，当生产主机发生故障时，可以直接由备机进行接管，而无需进行恢复操作，相比实时备份模式RTO≈0。云祺容灾接管模式提供了以下三种子模式：

模式一：实时备份+双机镜像

首先该模式要求备机的备用卷容量不小于生产主机备份卷容量，当启动备份时，实时监控数据在到达备份服务器后，备份服务器同时会将实时监控数据发送至备机，保证备机的备用卷和主机的生产卷数据完全一致；当主机故障时，通过手动将数据和应用无缝切换到备机。RPO ≈ 0。若无应用需要处理，则RTO ≈ 0，原理如2-6 所示。

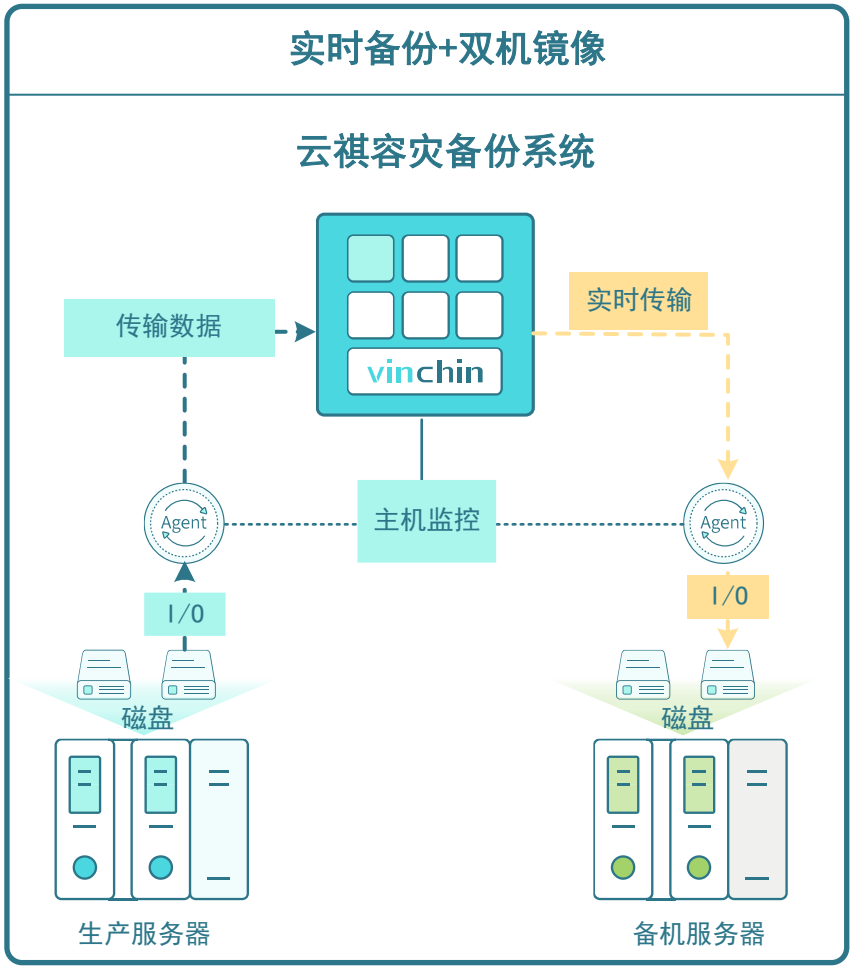


图 2-6 实时备份+双机镜像原理图

模式二：实时备份+自动接管

实时监控阶段的数据到达备份系统后，不会将实时监控数据发送至备机，当生产主机发生故障时，可通过自动挂载的方式将最新时间点的映射卷挂载至备机，并自动将数据和应用无缝切换到备机。由于接管数据实际上在备份服务器上，此容灾模式对备机的要求较低，只需能够运行对应版本的操作系统及应用即可，无需配置与生产主机对等的数据卷，但另一方面，接管后由于数据不在备机本地，性能会有所下降。RTO ≈ 0，RPO ≈ 0，原理如2-7 所示。

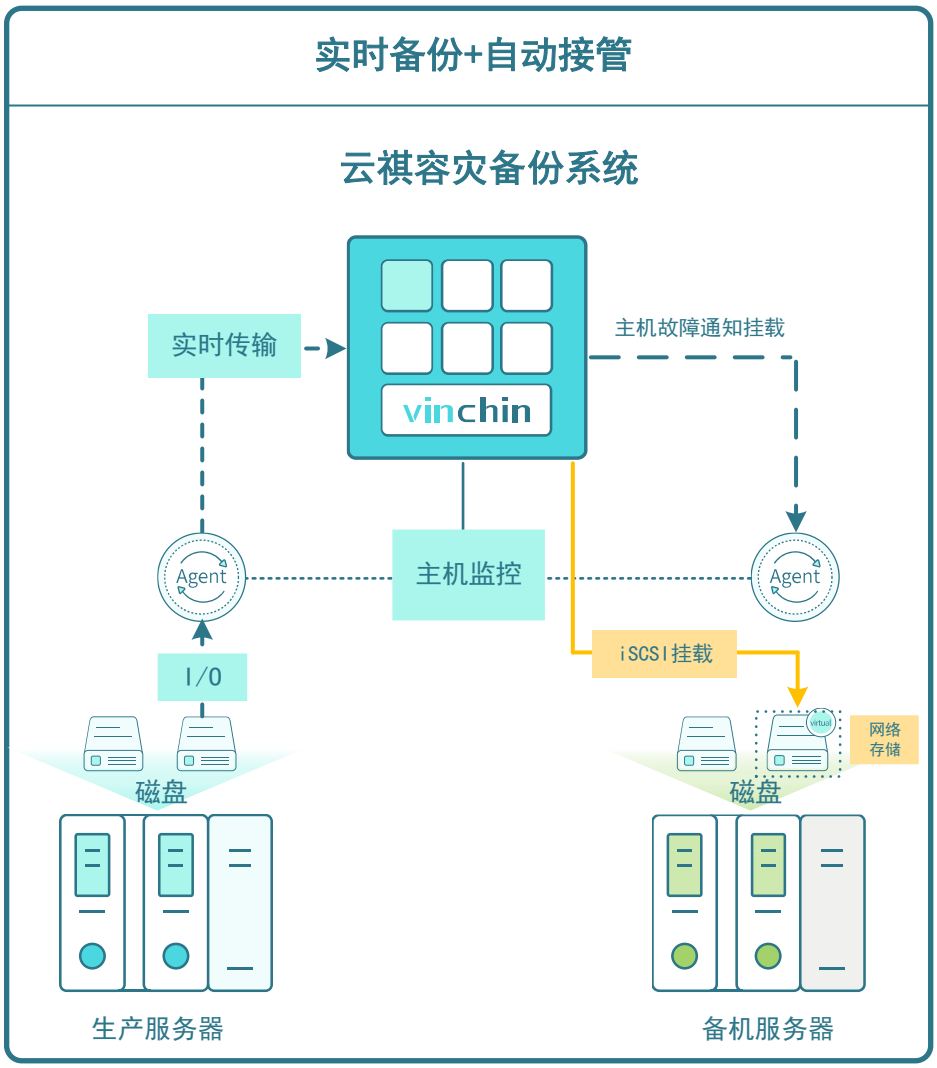


图 2-7 实时备份+自动接管原理图

模式三：实时备份+双机镜像+自动接管

首先该模式要求备机的备用卷容量不小于生产主机备份卷容量，备机的操作系统、应用名称及版本和主机的操作系统、应用名称及版本相同。主机端实时监控数据在到达备份服务器后，备份服务器同时会将实时监控数据发送至备机，保证备机的备用卷和主机的生产卷数据完全一。当生产主机发生故障时，直接使用备机中的数据进行接管，并自动将数据和应用无缝衔接。此模式下，因为接管数据本身在备机上，使用性能几乎不受影响。RTO ≈ 0，RPO ≈ 0，原理如2-8所示。

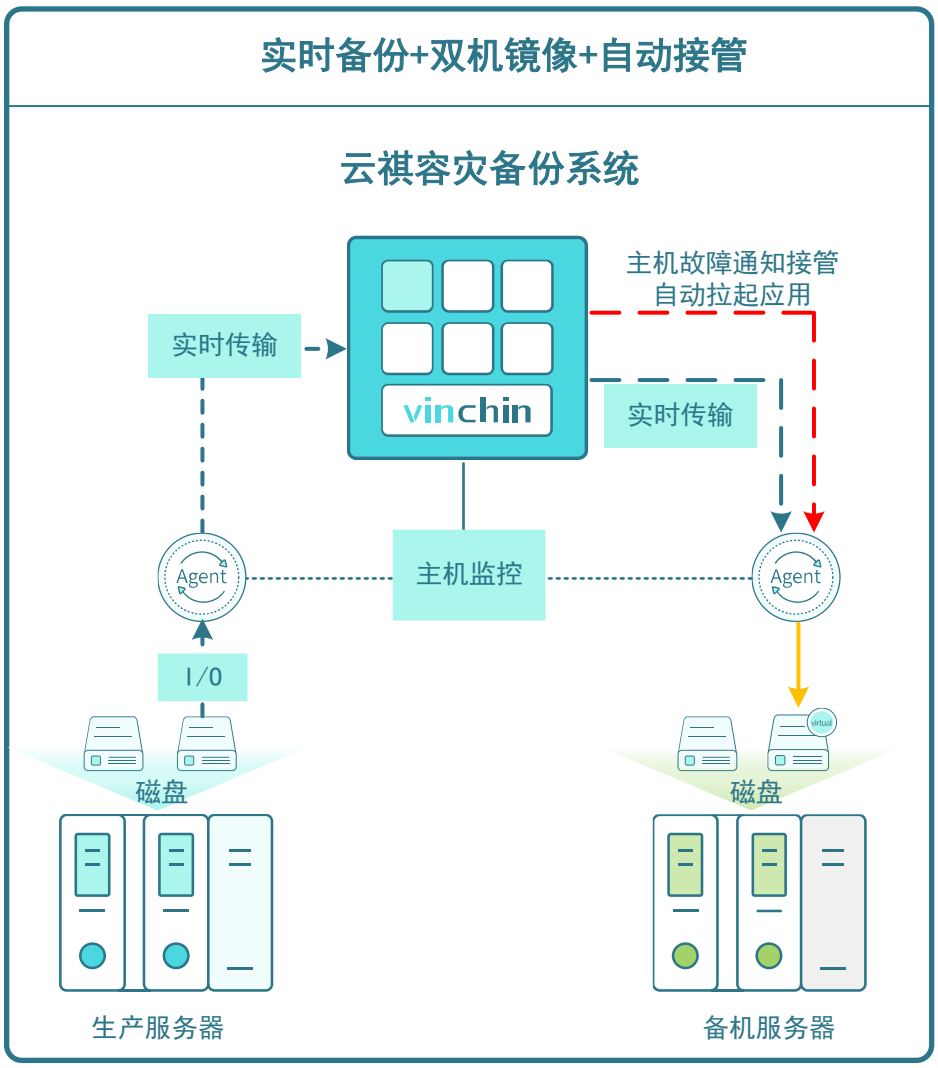


图 2-8 实时备份+双机镜像+自动接管原理图

实时容灾保护模块主要特点如下：

- **兼容性**：支持全平台 Windows 系统、支持 RHEL、CentOS 等 Linux 系统；支持主流存储介质和文件系统类型；
- **两种模式、满足不同需求**：支持实时备份和容灾接管两种任务模式；
- **安全性保证**：支持基于 AES256 的加密传输和存储数据加密；
- **有效数据提取**：能够从卷中提取有效数据，有效降低首次同步所需的时间；
- **断网续传**：在程序、生产主机重启，网络中断等情况下，支持断点续传功能，避免由上述异常情况引起需要重新同步的状况；
- **支持崩溃一致性处理**：通过数据一致性校验技术，可保障备份数据的完整性；
- **支持应用一致性**：通过标签点一致性技术，可生成和捕获无限数量的数据库一致性点用作恢复、接管；支持对操作系统事件的捕获并与持续备份数据关联；

- **任意时间点恢复**：实时备份模式和容灾接管模式下，均可支持最小 1 秒钟的任意时间点回退功能，有效避免人为误操作、病毒等非硬件故障引起的损失；
- **支持配置传输限速功能**：能够对单个任务进行传输限速配置；
- **支持异机**：支持将实时备份数据恢复到同架构下不同型号的硬件之上；支持在容灾接管模式下主备机硬件型号不相同；
- **主机级容灾**：支持在容灾接管模式任务运行中，通过心跳算法持续监测主机在线状态，当宕机或网络故障发生后，可自动或手动将业务接管到备机之上，并将主机 IP 切换至备机，从而实现主机级容灾的效果；
- **应用级容灾**：支持在容灾结果模式任务运行中，持续监测指定应用的运行状态，当监测到应用发生故障后，可自动或手动将应用故障前一刻的状态切换到备机上，由备机上的应用正常提供持续不间断的应用服务；
- **支持验证检查模式**：支持在容灾接管模式下，由管理员手动选择任意时间点进行接管；
- **数据库深度关联**：数据库作为主机环境中最重要的系统之一，实时容灾模块支持与数据库深度关联，在接管后用户无需对数据库进行额外操作即可正常使用；
- **支持一键切回操作**：当接管发生后，用户可在生产主机修复完毕之后执行一键切回操作，整个过程业务不会中断，回切完成后接管中变化的数据和应用状态将会从备机回到主机；
- **高度自定义的任务配置**：支持自定义接管到备机的挂载点，支持编写并执行接管触发时的检测脚本以及接管前后执行的自定义脚本，让管理员能够更好的结合自身 IT 环境，打造更加完善和可靠的容灾备份系统。

2.2. 虚拟机保护

得益于虚拟化技术给用户生产带来各种优势，用户IT环境中出现了大量的虚拟化软件，越来越多的核心业务系统部署或存放在虚拟化环境中。另一方面，由于技术发展，国内外涌现出许多开源或商业的虚拟化软件，而一些用户内部的生产环境中，同时存在多套从技术到架构都完全不同的虚拟化软件。因此，如何在复杂虚拟化环境中对重要数据进行备份和保护，是用户面临的一大挑战。

针对虚拟化备份云祺容灾备份系统采用无代理的模式（无需在虚拟机内部安装备份代理），通过多种备份传输链路对用户环境中虚拟机的磁盘映像进行备份，能够兼容目前市面上主流的虚拟化软件和云计算管理平台，同时能够提供兼容平台内的虚拟机互相进行到同构或者异构虚拟化平台的恢复，满足用户对复杂虚拟化环境中数据的备份需求。

虚拟机保护原理如下图2-8所示：

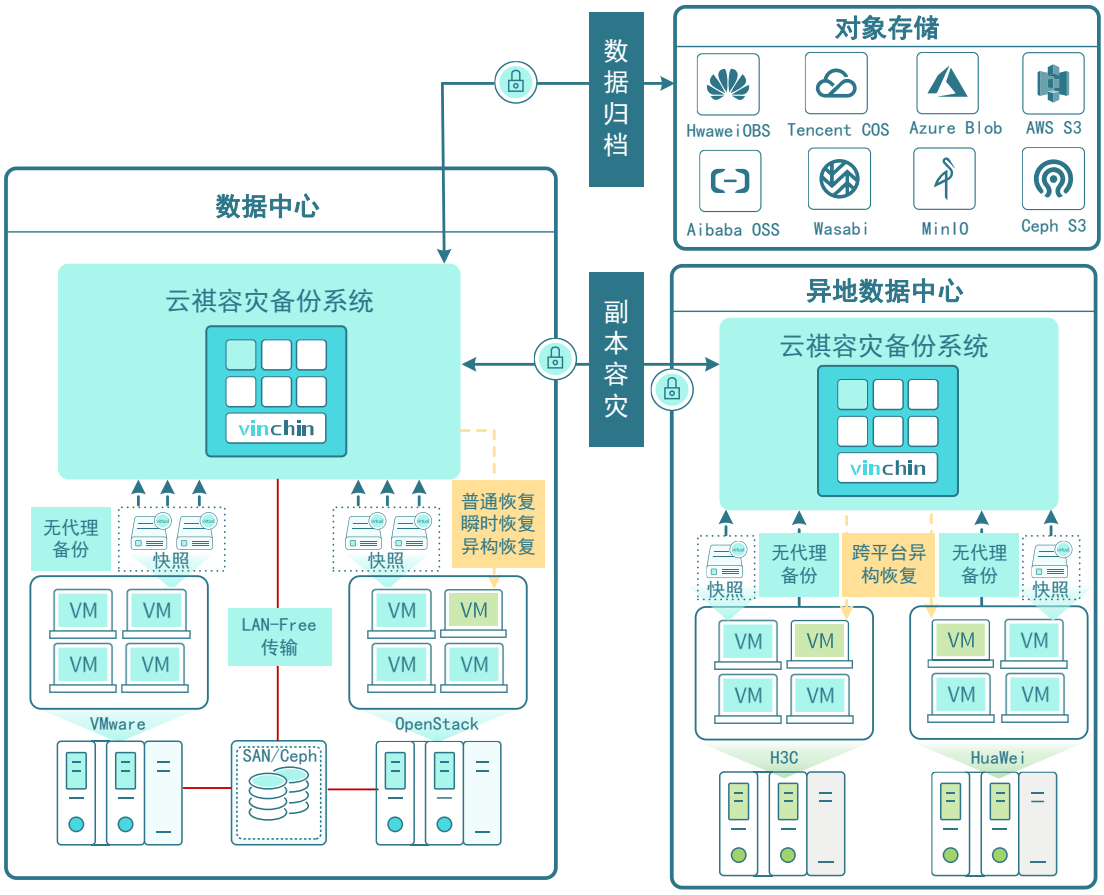


图 2-8 虚拟机保护模块原理图

云祺容灾备份系统虚拟机保护模块主要特点如下：

- **无代理备份**：无需在虚拟机内部安装备份代理；

兼容性：兼容VMware、Citrix Hypervisor、oVirt、深信服HCI、华为FusionCompute、

浪潮ICS、H3C CAS/UIS、ZStack、OpenStack等国内外常见虚拟化和云计算基础设施软件；

- **备份类型**：支持完全备份、增量备份、差异备份；
- **备份粒度**：虚拟机/磁盘
- **恢复粒度**：虚拟机/磁盘/虚拟机内的目录/文件
- **多种增量/差异计算方式**： 支持配置多种增量计算模式，以提高备份效率和降低备份存储空间占用。虚拟机保护模块支持的增量模式如表 2-1 所示。

表 2-1 虚拟机保护模块支持的增量模式表

增量模式名称	模式说明
普通模式	通过对比两次备份数据块的指纹进行对比，以计算两次备份之间的变化位图，该模式兼容性最强，但速度较慢
高速模式	云祺针对不支持 CBT 特性而提供的一种快速增量计算模式，起特点就是增量计算速度基本与 CBT/RCT 技术一致，缺点是每次备份结束之后都会保留一个快照，用于下次备份进行快速获取增量位图
CBT	即变化块跟踪技术（Change Block Tracking），是虚拟化平台针对快速进行增量备份提供的一种机制，能够在无需保留快照的情况下快速获取两次备份之间的增量位图

目前虚拟机保护模块针对每一类虚拟化/云计算平台支持的增量模式如表 2-2所示。

表 2-2 虚拟化及支持的增量模式对应表

虚拟化/云计算类型	支持的增量模式
VMware ESXi	CBT、普通模式（其中虚拟机 CBT 失效后程序自动切换为普通模式）
Citrix XenServer/Hypervisor XCP-NG	普通模式、高速模式、CBT（版本≥8.0）
Ovirt、RHV、OLVM	普通模式、高速模式、CBT（≥4.4.0）
深信服 HCI	普通模式、高速模式
浪潮 ICS	普通模式、高速模式、CBT（≥6.5.0）
H3C CAS/UIS	普通模式、高速模式
ZStack	普通模式、高速模式
OpenStack	普通模式、高速模式
Hyper-V	高速模式
云宏 CNWare Xen/Kvm	普通模式、高速模式
SmartX HCI	普通模式、高速模式
华为 FusionCompute	普通模式、高速模式、CBT

- **排除磁盘备份**：支持排除用户不需要备份的磁盘，如排除系统盘，只对虚拟机的数据盘进行备份；
- **永久增量**：支持永久增量功能，即只需第一次进行完全备份，后续持续执行增备，比需要定期生成完备点的方式更节省备份存储空间；
- **多种节省备份空间的手段**：通过配置“深度有效数据提取”、“重复数据删除”、“数据压缩”、“去零存储”等方法，有效降低备份数据存储空间的占用；
- **虚拟机瞬时恢复和在线迁移**（Hyper-V 不支持瞬时恢复）：无论是完备点还是增/差备点，无需合成即可执行虚拟机瞬时恢复任务，并且瞬时恢复任务启动时间基本恒定，时间不会随虚拟机大小或备份数据大小线性增长；
- **细粒度恢复**：结合瞬时恢复技术，支持无需进行虚拟机恢复即可恢复虚拟机内部的文件或者目录；
- **V2V 无代理跨平台恢复**：支持将备份的虚拟机数据恢复到异构的虚拟化平台之上，如将 VMware 的虚拟机备份数据恢复到深信服 HCI 之上；支持针对 OpenStack 平台上跨平台恢复后的虚拟机内部驱动自动替换，提高跨平台恢复成功率，减少人工干预；
- **可配置多线程并发传输**：能够在对单个虚拟机的单个磁盘进行备份/恢复时，采用多线程并发传输/读写的方式，适用于高带宽场景，极大提升任务执行效率；
- **可配置的高级恢复设置**：支持恢复时设置虚拟机名称、CPU 数量、内存大小、磁盘总线类型（跨平台情况下）、自定义 Mac/保留 Mac/自动生成 Mac 等配置；支持恢复某个指定的虚拟磁盘；
- **短期保留策略和长期保留策略结合**：短期保留策略支持按照时间和个数进行时间点保留，如保留 7 个时间点或保留最近多少天的时间点；长期保留策略采用 GFS（Granfather-Father-Son），可以支持按年，按月和按周保存关键完备点；

2.3. NAS 保护

NAS设备作为一套网络的附加存储，由于它使用方便、便于数据共享、相较于SAN和分布式存储价格相对适中，管理维护简单等因素，受到越来越多企业用户乃至个人用户的青睐，越来越多的用户数据存放在NAS设备中。但另一方面，随着数据集中存放，数据丢失的潜在风险也变得越来越高，因此用户对于NAS存储上数据备份的需求也日益高涨，且重视程度不亚于一些核心业务系统。

由于NAS本身提供的NDMP协议效率较为低下，针对目前海量数据存储的NAS设备而言，已不太适用。为此，云祺针对NAS设备采用了更高效的备份解决方案，其技术原理如图2-9所示，通过可视化界面配置完NAS设备和备份服务器的连通性后，将需要备份的目标目录通过NFS/CIFS协议挂载到备份服务器本地，然后通过NAS保护模块，快速的进行NAS数据的备份。当生产存储故障发生时，可将备份数据还原到新的NAS设备之上。

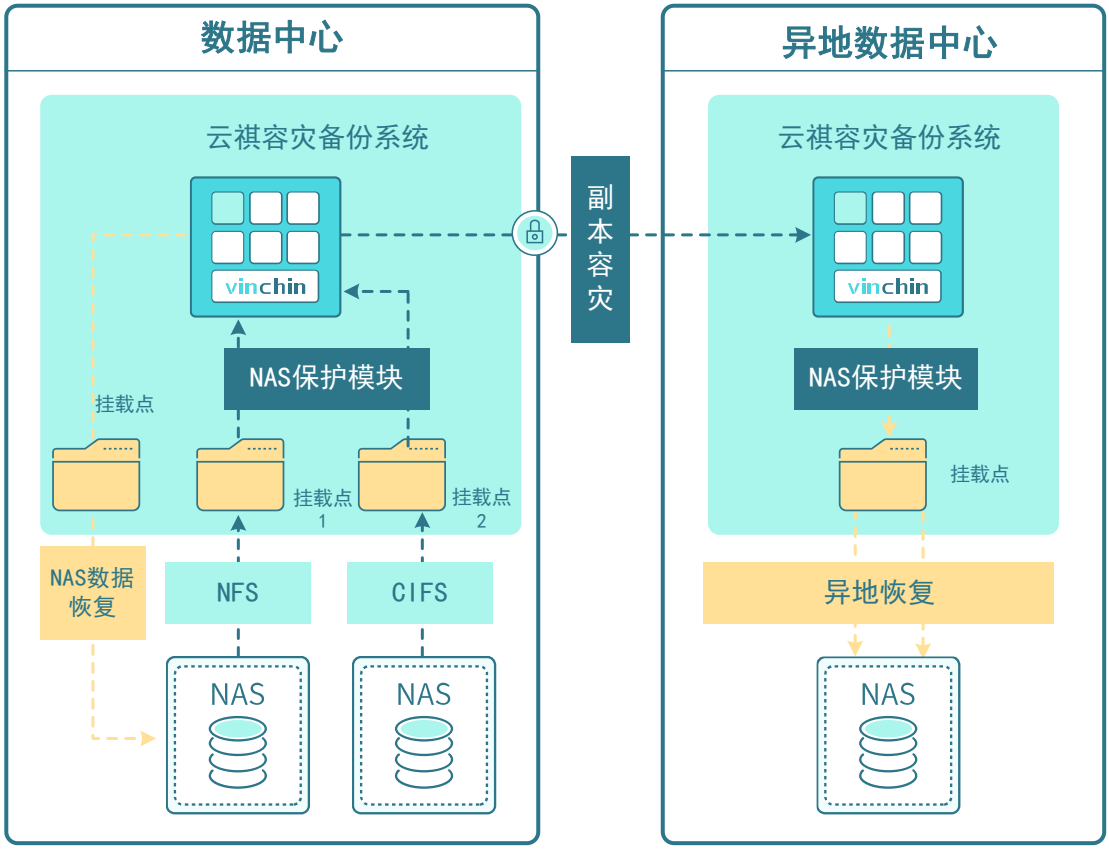


图 2-9 NAS 保护模块原理图

NAS保护模块主要特点如下：

- **兼容性**：支持通过 NFS、CIFS 两种协议进行挂载备份；可指定协议版本、访问权限（读写访问、只读访问）及其他高级配置参数；
- **备份类型**：支持完全备份、增量备份、差异备份；
- **排除匹配备份、指定匹配备份**：支持精确匹配和模糊匹配的排除/指定文件或子目录的备份功能；
- **备份数据存储配置**：支持配置基于 AES256 的备份数据存储加密；支持配置备份数据压缩功能；
- **并发配置及限速功能**：支持配置多线程提高备份/恢复效率；支持设置限速功能，降低备份/恢复对生产端造成的性能影响；
- **支持亿级海量文件/目录备份**：支持对上亿级的海量文件/目录备份和恢复支持；可通过对单个 NAS 设备配置多个备份/恢复任务、单个 NAS 任务内配置多线程并发提高海量数据备份/恢复的效率；
- **恢复方式**：支持源 NAS 设备上的覆盖恢复和新建恢复，支持异机 NAS 设备的恢复；

2.4. 备份数据 CDM

通过结合虚拟机瞬时恢复技术和虚拟化本身便于构建虚拟网络的特性，云祺容灾备份系统特别推出备份数据CDM模块。备份数据CDM模块通过在虚拟化环境中构建隔离网络，在不影响生产应用正常运行的情况下，周期性的通过瞬时恢复技术使用最近的时间点启动虚拟机，并且对启动的验证虚拟机进行各种完整性和正确性验证。

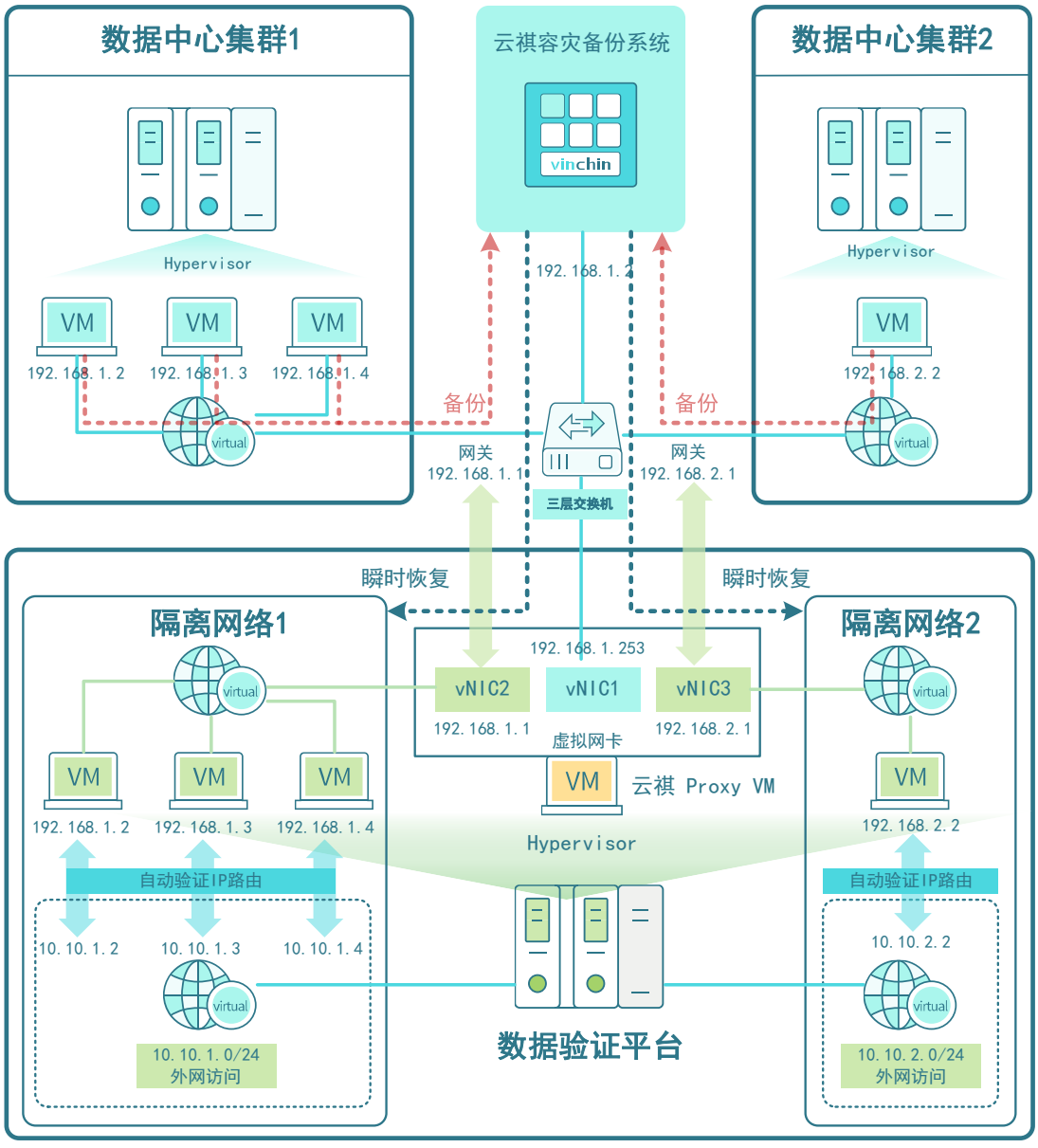


图 2-10 备份数据 CDM 原理图

以2-10为例，用户虚拟化环境存在两台主机，分别为Host1和Host2，二者分别在两个不同的网段，Host1位于生产192.168.1.0/24，Host2位于生产192.168.2.0/24，中间通过一台三层交换机连通，两个接口分别为2个网段的网关。

当自动验证任务运行后，备份系统会在Host1所在的虚拟化环境中构建如下内容：

1. **云祺ProxyVM**：作为隔离网络和生产网络的消息转发器，在隔离网络中伪装为生产网络的网关；

2. **一个虚拟二层交换机和对应端口组**：用于构建隔离网络内部的二层网络；

3. **瞬时恢复的VMs**：验证备份数据的主题，由配置任务的最新VM时间点生成；

4. **增加备份服务器路由表规则**：确保备份服务器能够通过Proxy VM与隔离网络内部虚拟机通信；

上述资源构建完成后，系统将会自动进行备份数据的验证，备份系统会根据内置的路由表，通过Proxy将消息转发到隔离网络内的瞬时恢复虚拟机，因为隔离网络内的瞬时恢复虚拟机网关配置与源环境相同，通过Proxy VM伪装生产环境网关后，即可正常与备份服务器进行通信。

备份数据CDM模块具有以下特点：

- **不影响生产环境网络架构**：由于采用构筑隔离网络的方式进行自动验证，整个环境中只有备份系统可以与隔离网络内的虚拟机进行通信验证，不会对用户生产环境造成网络冲突、业务冲突的影响；
- **效率较高、生产存储空间占用可忽略不计**：由于瞬时恢复的虚拟机由瞬时恢复技术创建而来，无需将备份数据回传至用户生产存储，因此不会占用生产空间进行，且任务启动速度极快。生产存储上仅需消耗一个经过云祺定制的小型系统，即 Proxy VM；
- **在源环境和新环境进行自动验证**：任务可指定在源生产主机之上，也可以使用异机进行备份数据自动验证；
- **自动验证备份数据**：支持配置每天/每周/每月三种策略，任务会根据启动时间自动从关联的 VM 备份任务获取时间点进行备份数据自动验证；
- **按需启动自动验证**：可根据用户实际需求，按需手动执行任务进行备份数据验证；
- **简化网络配置**：为降低配置门槛，备份系统会自动生成当前环境下尽量可用的隔离网段和映射地址，同时支持生成后用户手工自定义配置隔离网络和路由关系；
- **虚拟机按照应用分组**：支持将备份任务内的虚拟机按照应用分组，以分组方式创建验证任务；
- **多种验证方式**：默认支持网络连通性检测、虚拟机运行状态检测、屏幕截屏检测等检测方式；
- **可视化报表功能**：每次验证的结果可采用可视化的图形报表进行输出，便于用户进行结果查看和审计；

2.5. 副本及归档

为避免备份数据存在单点故障问题，云祺容灾备份系统支持副本和归档功能。副本和归档功能原理如图 2-7所示。

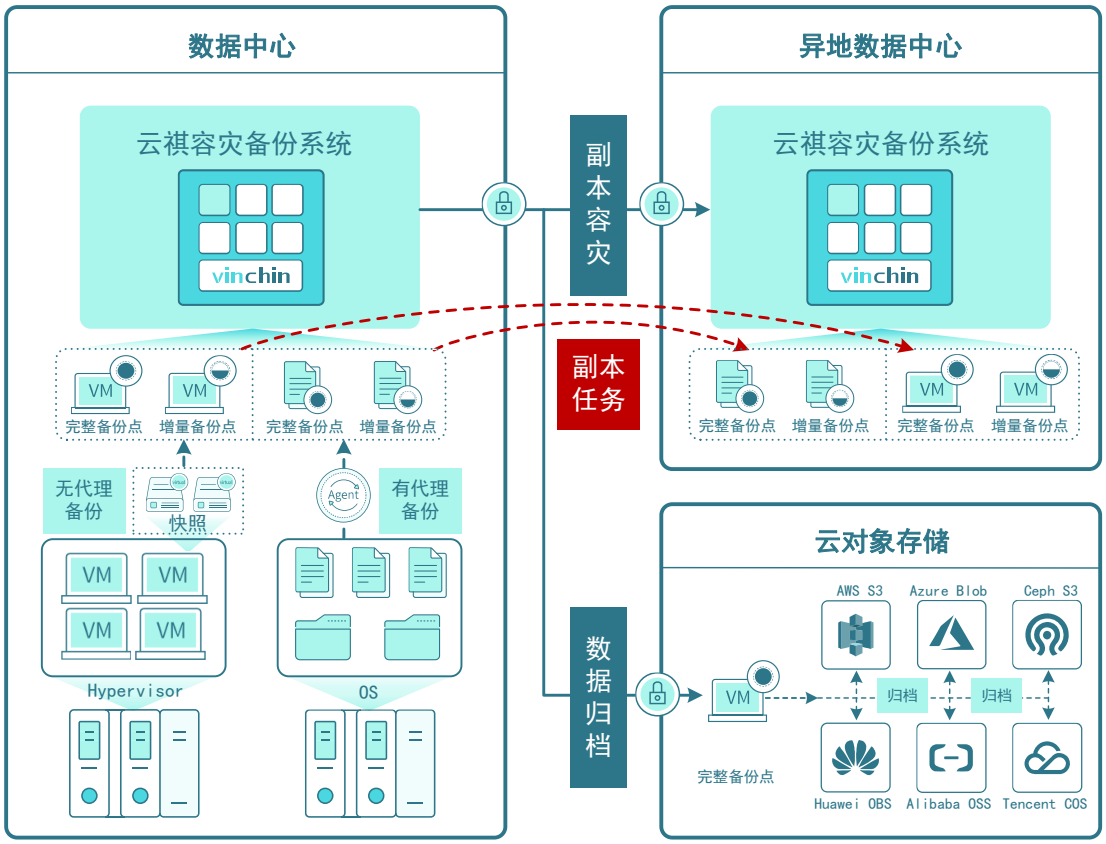


图 2-7 副本及归档功能原理图

其中，副本功能会将备份链完整同步到目标存储或者异地灾备中心，而归档任务每次完成后会在目标介质上生成1个完备点。无论是副本数据或归档数据，都可以直接用于对应模块的恢复或瞬时恢复功能。

副本和归档功能具有以下特点：

- **副本功能的模块**：文件保护、数据库保护、操作系统保护、虚拟机保护和 NAS 保护模块支持副本功能；
- **归档功能的模块**：操作系统保护模块和虚拟机保护模块支持归档功能；
- **副本功能支持的目标类型**：支持副本到本地 NAS、SAN、DAS 存储，支持副本到异地备份系统；
- **归档功能支持的目标类型**：支持归档到本地 NAS、SAN、DAS 存储，支持归档到异地备份系统，支持归档到包括 AWS S3、Microsoft Azure、阿里云、腾讯云等国内外知名云存储之上；
- **数据拉回功能**：支持将副本/归档到异地或者云存储上的数据拉回到本地备份系统；

- **断点续传**：支持在副本过程中，网络中断或者服务重启后从已处理的备份点继续进行断点续传；
- **高级网络配置**：支持压缩传输，加密传输功能；
- **副本/归档数据时间保留策略独立**：副本和归档任务拥有自己的保留策略，可以不需要按照源任务或数据的保留策略进行设置，例：本地备份保留 7 个点，异地副本或归档任务保留 14 个；
- **灵活的源数据关联模式**：支持直接选择指定时间点进行归档或副本，支持与备份任务进行关联。副本任务会在任务启动后将上次任务到本次任务之间新增的时间点复制到指定位置；归档任务会在任务启动后通过在线合并技术，在目标位置生成一个完备归档点。

3. 关键技术

3.1. 永久增量

3.1.1. 概述

按照传统的增量备份方式，一般会周期性的进行完备，以减少备份链的长度，也便于保留策略删除过期数据，以此释放备份存储空间。由于需要进行周期性的完全备份，传统方法会存在以下几个问题：

1. 空间占用较大：假设保留N条备份链（一个完备和多个关联增备点的组合），每条备份链有M个增量点，则备份空间至少需要（N+1）个完备点的大小和 N×M个增量点的空间，这是因为只有生成第N+1个点的时候，才能把第一条备份链进行删除；

2. 备份效率低：由于需要周期性的在数次增备之后执行完备，必然会导致整体备份效率下降，过大的备份窗口可能会影响后续的正常增备，并且可能影响生产环境的运行；

3.1.2. 技术原理

云祺容灾备份系统采用永久增量技术以解决传统方案存在的问题，该技术的主要原理逻辑如下图3-1所示，具体流程如下：

1. 假设某个任务配置了保留3个备份点，T0时刻开始进行第一次完备；

2. T1到T2时刻开始进行两次增量备份；

3. T3时刻任务执行后，备份链上存在1个完备点和3个增备点，由于设置了保留3个备份点的策略，此时备份系统会检测到需要执行保留策略，需要删除T0时刻的数据，但是由于T0

时刻为完备点，后续增量点会依赖于该完备点，因此系统会执行下面三个操作，完成T0时刻时间点的删除；

- 将 T1 的数据和元数据合并到 T0 时刻中；
- 将 T0 修改为 T1,；
- 将 T2 的父时间点设置为新的 T1。

4. 完成后备份链存在T1~T3三个时间点，T1从增备点变成完备点，整个保留策略执行完成。

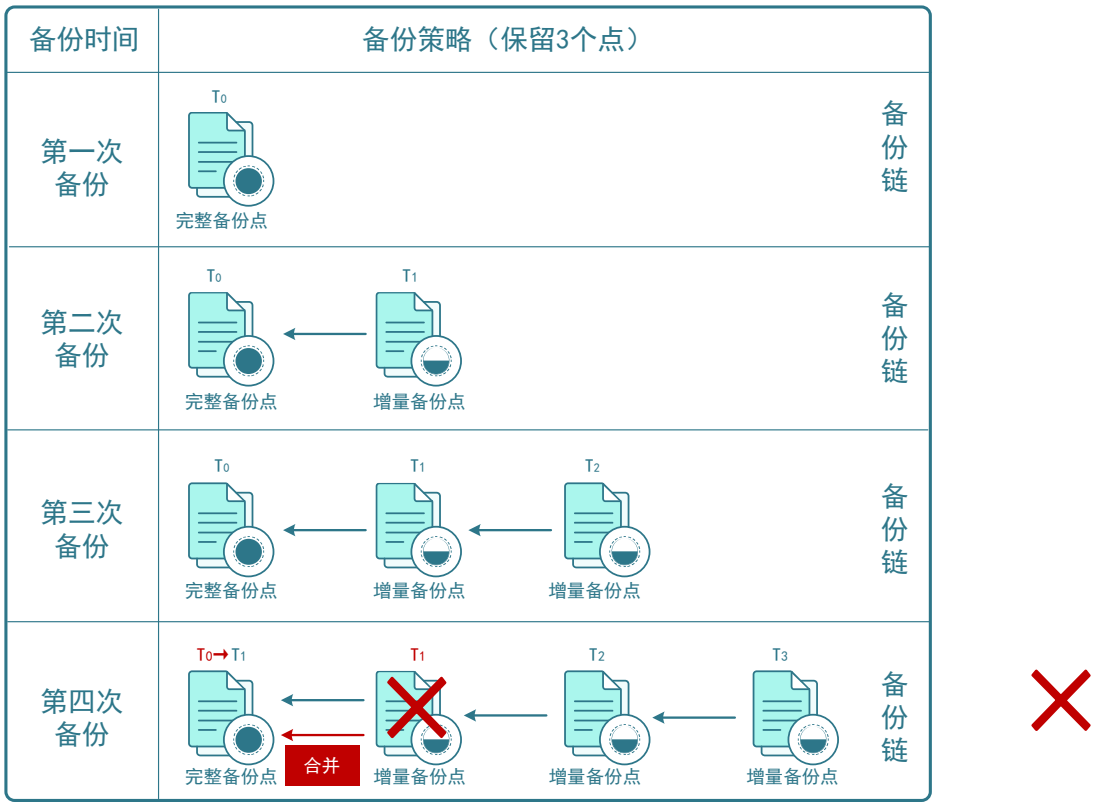


图 3-8 永久增量技术

3.1.3. 技术特点

由于支持增量点合并，保留策略可以有效处理备份链中删除完备点的操作，因此首次完备之后，只需执行增量即可。其特点如下：

- **提高备份效率**：由于只需首次备份执行完全备份，备份效率整体提升显著；
- **降低备份存储空间**：备份存储空间只需要 1 个完备大小加 N-1（其中 N 为保留时间点个数据）个增备大小即可备份容量需求；
- **异地副本功能保留策略独立的基石**：通过该技术，副本数据链和本地备份链结构和长度可以不相同；

• **可搭配重复删除和压缩功能**：由于将备份数据拆分为索引数据和实际数据两部分，该数据组合同样是重复数据删除和压缩实现的基础，进而进一步减少备份空间.

3.2. 瞬时恢复

3.2.1. 概述

瞬时恢复，利用生产服务器计算资源、备份系统存储资源、备份数据，运行虚拟机，达到在数分钟以内恢复虚拟机运行的目的。

操作系统在虚拟机内启动时，一般只需要读写数百兆至数GB数据。云祺容灾备份系统通过瞬时恢复技术，将任意一个备份数据虚拟为完全备份，提供给虚拟机使用。在千兆网络环境下，可将启动操作系统的数据全部传送到生产服务器，实现瞬时恢复。

瞬时恢复不需要将所有的备份数据全部传输到生产服务器，而只传输启动操作系统、应用所必须的数据，大大提高了恢复效率，加快了应用恢复速度。该技术也是作为备份数据CDM的核心技术之一。

3.2.2. 技术原理

瞬时恢复主要分为瞬时恢复阶段和在线迁移两个阶段，具体原理如图 3-9所示。其中瞬时恢复阶段流程和原理如下：

1. 任务启动会创建用于瞬时恢复虚拟机写入的缓存；

2. 在目标虚拟化上创建用于瞬时恢复的NFS存储；

3. 通过瞬时恢复技术让虚拟化平台看到一个完整的磁盘文件，构造出的磁盘文件基础上创建瞬时恢复虚拟机，该磁盘文件实际数据来源于备份链和瞬时恢复缓存；

4. 虚拟机创建完成之后，瞬时恢复虚拟机即可正常运行使用，可用于数据验证、测试和应急业务接管；

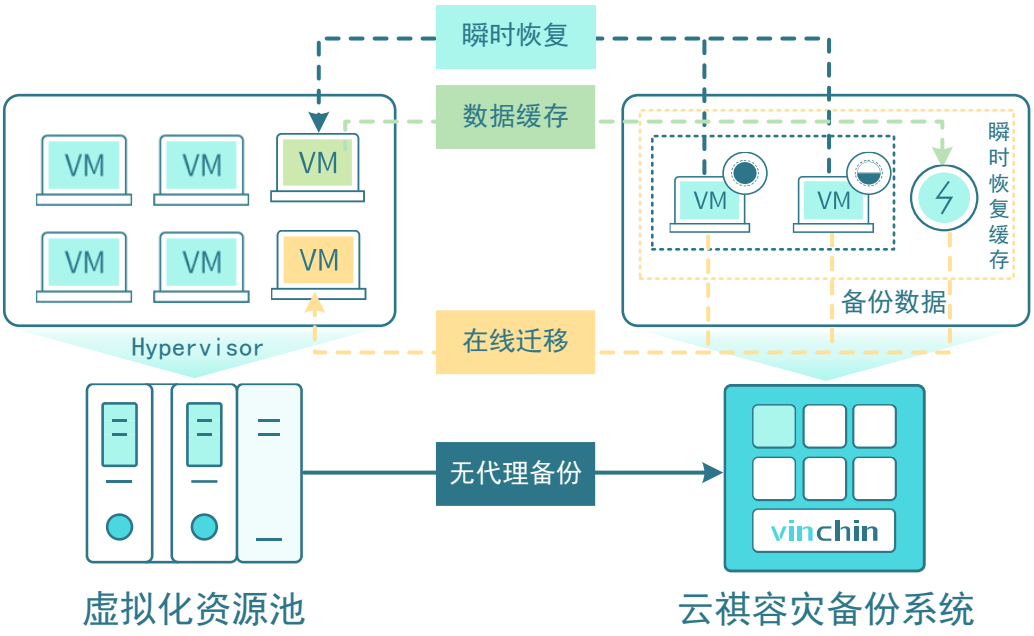


图 3-9 瞬时恢复技术原理图

在线迁移流程及原理如下：

1. 启动在线迁移任务之后，会在目标集群或主机上创建一台新的虚拟机，记VMmigration，而瞬时恢复虚拟机记VMinstant。

2. 备份系统会先将瞬时恢复任务对应的备份时间点数据恢复至VMmigration；

3. 瞬时恢复缓存内的新增数据会通过迁移技术进行恢复，在缓存恢复到仅剩一小部分内容的时候，会关闭VMinstant，确保缓存不会再有新增数据后，将剩余数据恢复到VMmigration之上；

4. VMinstant和VMmigration数据完全相同之后，就可以启动VMmigration电源，业务即可完全回到生产环境之中，继续正常为用户提供服务；

3.2.3. 技术特点

- **备份系统无需合成时间点**：瞬时恢复选定的时间点，无论是完备或增备，在启动任务过程中间无需合成时间点，任务启动时间不会随大小线性增长，趋近恒定值；
- **备份数据无需快照创建操作**：由于采用独立缓存空间的方案，无需通过快照机制，也可瞬时恢复 VM 产生的数据写入不会对源备份数据造成破坏。
- **兼容跨平台虚拟化瞬时恢复**：瞬时恢复的备份数据来源可与当前虚拟化目标异构，如将 VMware 的备份数据作为源，在深信服 HCI 上启动瞬时恢复任务；
- **在线迁移功能**：提供在线迁移功能，用户可用瞬时恢复功能进行业务的应急接管，而后通过在线迁移功能逐步将数据从备份系统回迁至生产资源之上。

- **其他高级功能的基础：**为细粒度功能、备份数据 CDM 功能的技术基础之一。

3.3. 深度有效数据提取

3.3.1. 概述

文件系统作为计算机操作系统最主要的存储设备上的文件数据结构组织方法，其极大方便了用户日常对计算机的使用。而针对虚拟机的磁盘映像进行备份的通用技术，基本上都是采用识别虚拟机磁盘文件元数据、通过虚拟化API（如CBT接口）或者分区结构提取位图进行备份。由于虚拟化底层无法感知文件系统内部进行文件删除的操作，因此随着时间推移，完全备份的有效数据会越来越大，最终趋于整个磁盘的大小。

深度有效数据提取技术的提出，就是为了解决上述方案的缺陷，能够准确识别磁盘内的实际使用的数据。整体来看，该技术能够有效减少备份的传输大小和存储大小，不但能够节省空间，还可以提升整体备份效率。

3.3.2. 技术原理

深度有效数据提取技术的核心原理为穿透块设备层，直接识别磁盘内的分区信息和文件系统信息，从而解析出文件系统层有效数据位图。通过将传统备份方式的有效数据位图进行结合，生成新的备份数据位图，从而达到减少备份数据大小的目的。目前深度有效数据提取功能支持排除已在文件系统中删除的数据块、交换文件块以及分区间隙块等无需数据块。

目前该技术应用于虚拟机保护模块、操作系统保护模块，具体原理和逻辑见图 3-10。其中，虚拟机保护模块中深度有效数据技术的应用逻辑如下：

1. 在备份任务阶段完成基本信息获取及快照创建之后；

2. 虚拟机保护模块按照目标虚拟化对应的方法获取磁盘的有效数据位图（如VMware的CBT接口返回的位图信息）；

3. 通过深度有效数据提取引擎获取对应虚拟磁盘的磁盘位图；

4. 备份系统通过将步骤2和3得到的两个位图进行处理，生成新的位图；

5. 虚拟机保护模块会使用新的位图信息进行对应数据的备份传输；

从图 3-10中可以看出，操作系统保护模块通过引擎获取之后，直接使用该位图文件进行识别和数据传输。

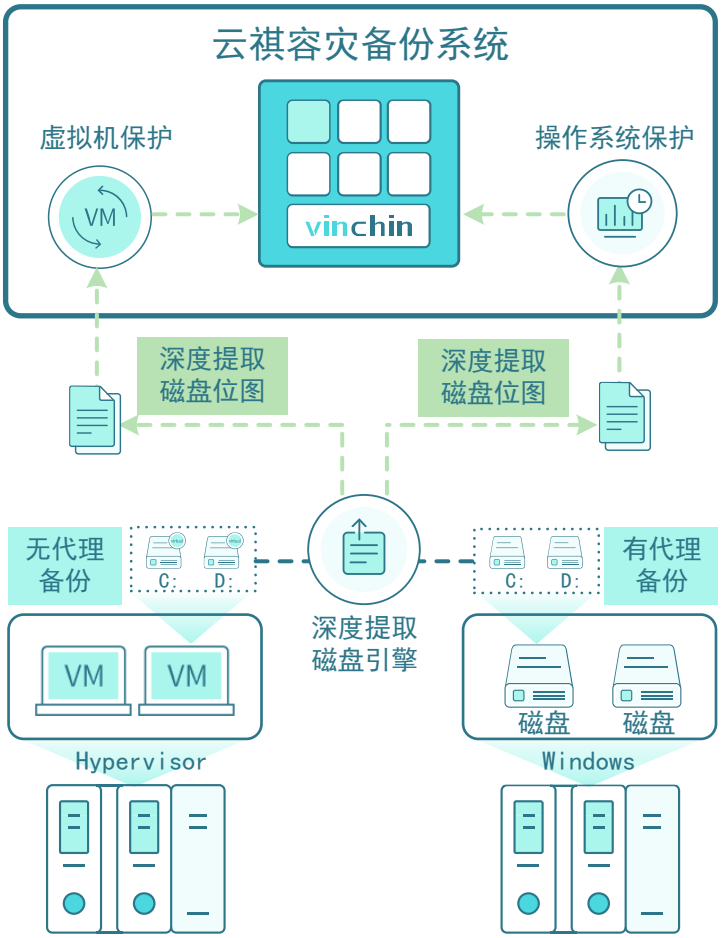


图 3-10 深度有效数据提取原理图

3.3.3. 技术特点

- **深度解析磁盘结构、提高备份效率**：不依赖虚拟化本身提供的位图解析功能，无论 CBT/RCT 是否失效，都能够有效提高备份效率降低备份数据大小；
- **灵活深度有效数据提取配置**：开启深度有效数据提取功能时，默认会自动排除被文件系统标记的已回收块，同时支持设置“排除分区间隙”和“和排除交换文件块”等两个高级选项，用户可根据自身需求进行开启或关闭。

3.4. 任意时间点回退

3.4.1. 概述

任意时间点回退由实时数据捕获数据技术、逆向增量技术等作为支撑。其作为CDP这一概念的核心技术之一，解决了传统镜像系统和实时同步复制存在不可低于软件故障的问题（解释：因为软件故障、人为误操作等会落盘，同样会被镜像技术同步到备机或镜像文件中），为用户提供了“后悔药”。

3.4.2. 技术原理

图 3-11为云祺容灾备份系统实时容灾保护模块中任意时间点回退的技术原理，以下通过四部分内容进行阐述：

- **实时变化数据的捕获**：实时保护模块代理安装在用户生产主机之上，代理通过内核层实时捕获生产磁盘的所有 IO，一旦捕获写请求，即将数据通过应用层发送至备份服务器，此技术可保证 RPO 接近 0；
- **存储空间结构**：针对每个被监控的卷，都会划分与之对应的镜像空间和日志空间，由于使用逆向增量技术，首次同步完成后，在任务实时监控阶段，会确保镜像空间数据与生产卷内容完全一致；而日志空间，由监控过程中通过 Copy-On-Write 机制生成的逆向增量数据组成；
- **实时备份恢复任意时间点回退**：在实时备份模式下，当灾难发生需要将数据恢复至新主机时，并制定某个时间点 T 时，首先系统会先从日志空间中将逆向增量的内容恢复至目标卷，然后通过位图将未恢复块的内容从镜像空间取出，并进行恢复，最终目标主机恢复到用户指定 T 时刻的状态；
- **容灾接管模式任意时间点回退**：相比实时备份模式，实时接管模式逻辑相对简单，由于备机磁盘内存储数据与生产主机一致，因此当用户需要进行回退操作时，备份系统只需要回退数据从日志空间取出，发送至备机即可将主机状态回退到指定时间；

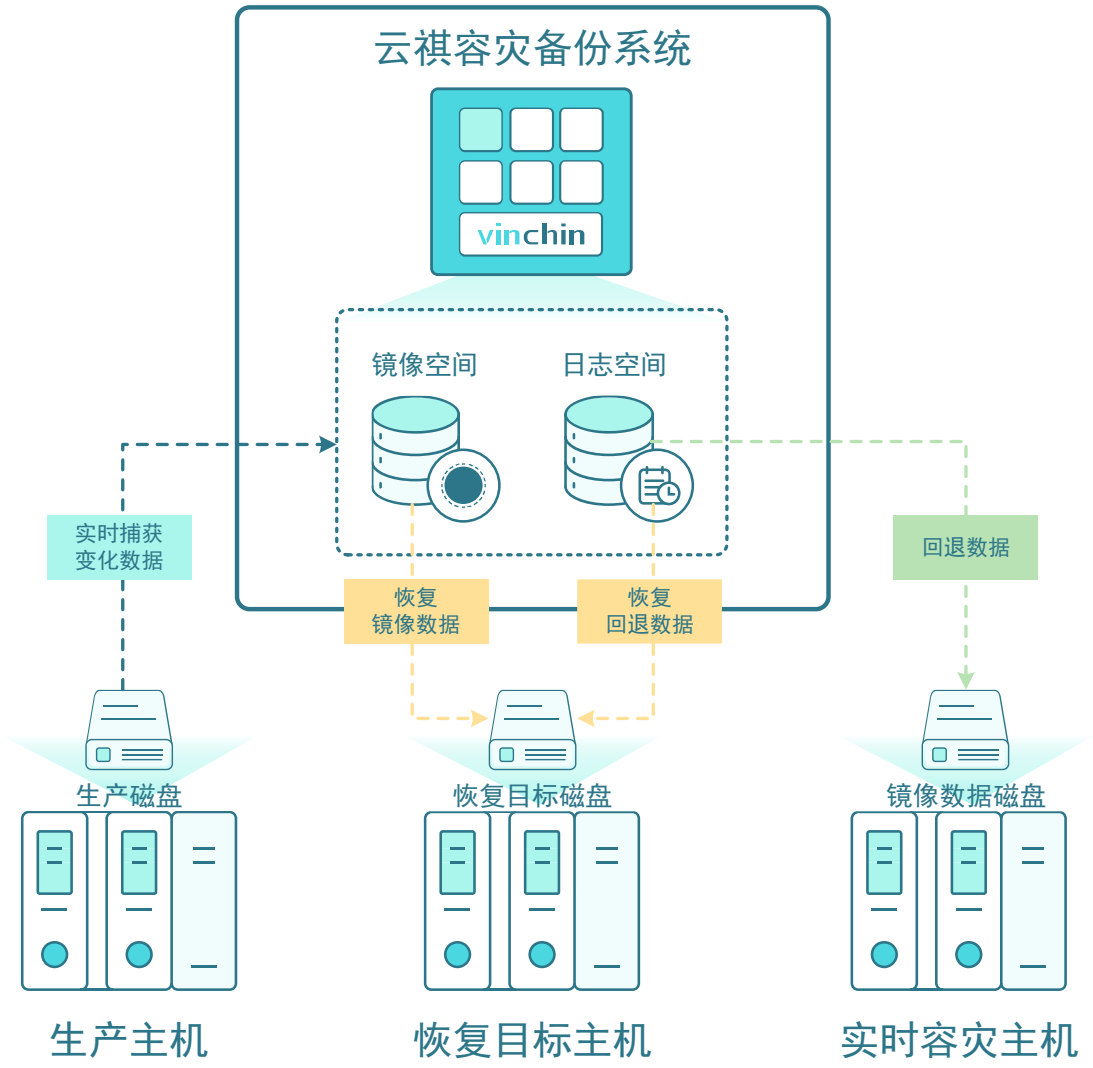


图 3-11 任意时间点回退技术原理

3.4.3. 技术特点

- **真正的实时方案**：采用 I/O 实时捕获技术，无需进行增量计算即可获取变化数据；
- **存储空间按需增长，支持加密压缩**：镜像空间和日志空间无需预先分配存储空间，采用按需分配模式；存储结构能够有效兼容压缩、加密等功能；
- **保留策略**：支持按照天数的保留策略，可以回收过期的日志空间数据；
- **逆向增量存储结构**：采用逆向增量存储模式，回退效率高；
- **高效的回退算法**：内置的高效数据定位和回退算法，能够快速确定回退点，并且在回退过程中，能够确保磁盘中每个编号的数据块，最多只会进行一次写操作，保证回退恢复数据量最小化。

3.5. 海量文件备份

3.5.1. 概述

随着科技的发展与进步，数据呈现爆炸式增长，网上的社交、通信、视频、商务、实验、医疗等等应用往往能产生几亿、几十亿，甚至几百亿的文件。数量庞大，体积小的文件给管理、访问性能、存储效率等方面带来了巨大的难题，同时使得文件备份的效率大幅降低，极大的提升了数据保护的难度和灾难发生恢复的效率。

传统文件备份技术方案流程需要经历目录结构扫描和数据传输两个主要步骤，假设扫描时间为N，数据传输为M，则上述两个主要阶段串行时间为N+M，而针对海量文件备份N的时间开销也可能很大，甚至大于传输时间M。

3.5.2. 技术原理

云祺容灾备份系统提供了一套能够兼容主机和NAS环境海量文件备份的机制，通过以下几个方式优化备份效率，降低海量文件的备份时间：

- 采用生产者消费者模型进行备份，扫描及数据传输流程合并，即边扫描边传输；
- 并发数据传输，提高带宽利用率；
- 合并小文件传输，减少网络交互；

海量文件备份技术原理见图 3-12：

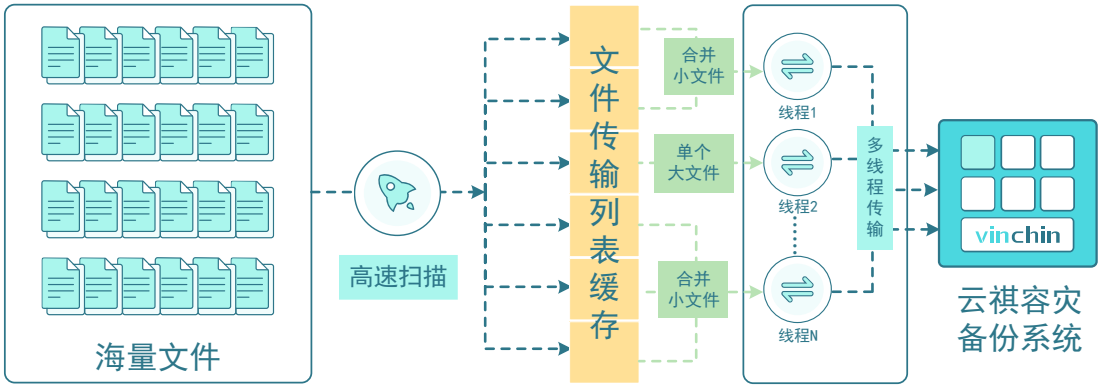


图 3-12 海量文件备份技术原理

3.5.3. 技术特点

通过云祺海量文件备份技术的机制，相比传统技术方案，时间开销完成了从1+1=2到近乎1+1=1的转变，有效的提高了海量文件备份场景的效率，降低了整个备份时间窗口，让用户可在同样时间范围内获得更多可用的恢复点，有效降低RPO。

3.6. 重复数据删除和压缩

3.6.1. 概述

云祺容灾备份系统通过结合数据切片、源端去零传输和存储、重复数据删除技术和压缩相结合，能够有效降低备份数据在物理存储上的存储空间。

相关技术均采用软件方法进行实现，不依赖于底层硬件，因此可以有效应用于各种硬件和环境和后端存储设备。

3.6.2. 技术原理

完整的流程及原理如下所示：

1. 先对源数据进行切片分块；
2. 数据传输前确定是否为零数据；
3. 备份系统接收到数据包后，如果带有零标记，则直接记录索引，然后处理下一个数据块；
4. 如果为非零数据块，则检测当前任务是否开启了重删功能，如果未开启，则进入步骤5；如果开启重删则进行以下操作：
   a) 通过hash算法计算数据块指纹；
   b) 将计算出的指纹放入指纹库中查找，确认是否有已经存在的数据块；如果找到匹配，则直接从指纹库中找到的数据块元数据取出，并更新到当前索引之中，并进行下个数据块处理。
   c) 如果未找到匹配，则将指纹和数据库元数据加入指纹库，则进入步骤5
5. 确认是否开启了压缩功能，如果开启了压缩功能，则对数据块压缩之后，存储数据块并更新索引文件；如果未开启，则直接存储数据块，并且更新元数据文件。

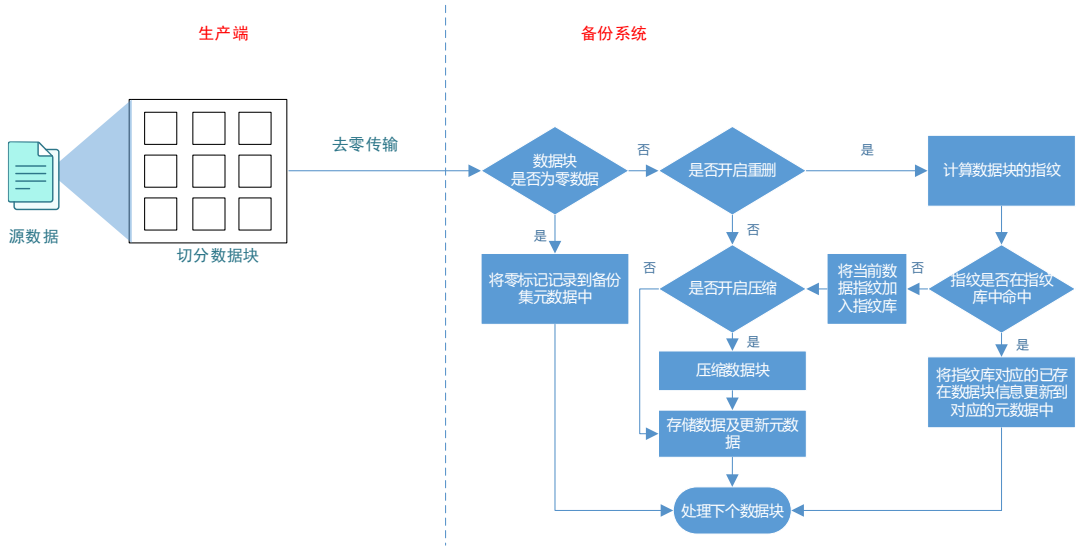


图 3-6 重复数据删除和压缩技术原理

3.6.3. 技术特点

- **采用数据块切片模式**：能够有效适应于虚拟机、操作系统等块级的数据空间节省；
- **灵活的存储空间节省配置设置**：可针对单个备份任务设置是否开启重删、压缩功能；
- **高效的压缩效率**：目前采用的压缩算法能够在空间和时间上取得较好的平衡，单线程情况下开销约为 10%左右；
- **去零传输和存储**：在数据传输和存储前支持零数据块检测，能够高效节省零数据对存储空间的占用，并且有效避免零数据造成的额外压缩、重删计算开销；

4. 多租户

4.1. 功能介绍

随着云计算的不断发展，云计算相关技术已经得到了极大的普及和应用，越来越多的用户选择将应用、系统迁移至在各类云环境之中。但是在整个过程中，需要面临各种各样复杂的问题，如平台选择、系统迁移、多云管理、应用优化以及成本核算和安全管理等问题。云MSP（Cloud Management Service Provider，即云管理服务提供商）就是为了解决该问题而诞生的专业团队。通常是指对接一家或者多家公有云服务厂商，为企业提供上云、开发、迁移、代管、运维、容灾备份等专业服务，根据Gartner的定义，MSP应该具备三大能力：CMP（Cloud Management Platform，云管理平台）、托管服务以及专业服务（咨询和实施）。其中CMP除了需要对接云计算基础设施，还需要对接容灾备份软件，以此为云环境的终端

用户的可靠数据和应用保障。

为此，云祺容灾备份系统提供了一套能够满足云环境和MSP需求的多租户机制，该机制主要通过以下几个方面实现：

- 增加租户概念；
- 租户内采用角色、用户组、用户的权限管理体系，详情可参考章节 5.1；
- 备份系统内部对象资源化，资源可分配；
- 增加计费功能；
- 提供备份系统 REST API，方便集成进 CMP 环境中。

通过上述内容的增加，备份系统可以很好的适用于各类云环境，多租户功能和机制可以满足MSP对其客户进行租户划分，资源划分以及计费划分，同时备份系统提供的API可以让备份系统更好跟CMP系统进行集成，能够有效完善MSP为用户提供容灾备份服务的能力。

4.2. 实现原理

图 4-13为备份系统多租户的逻辑架构。

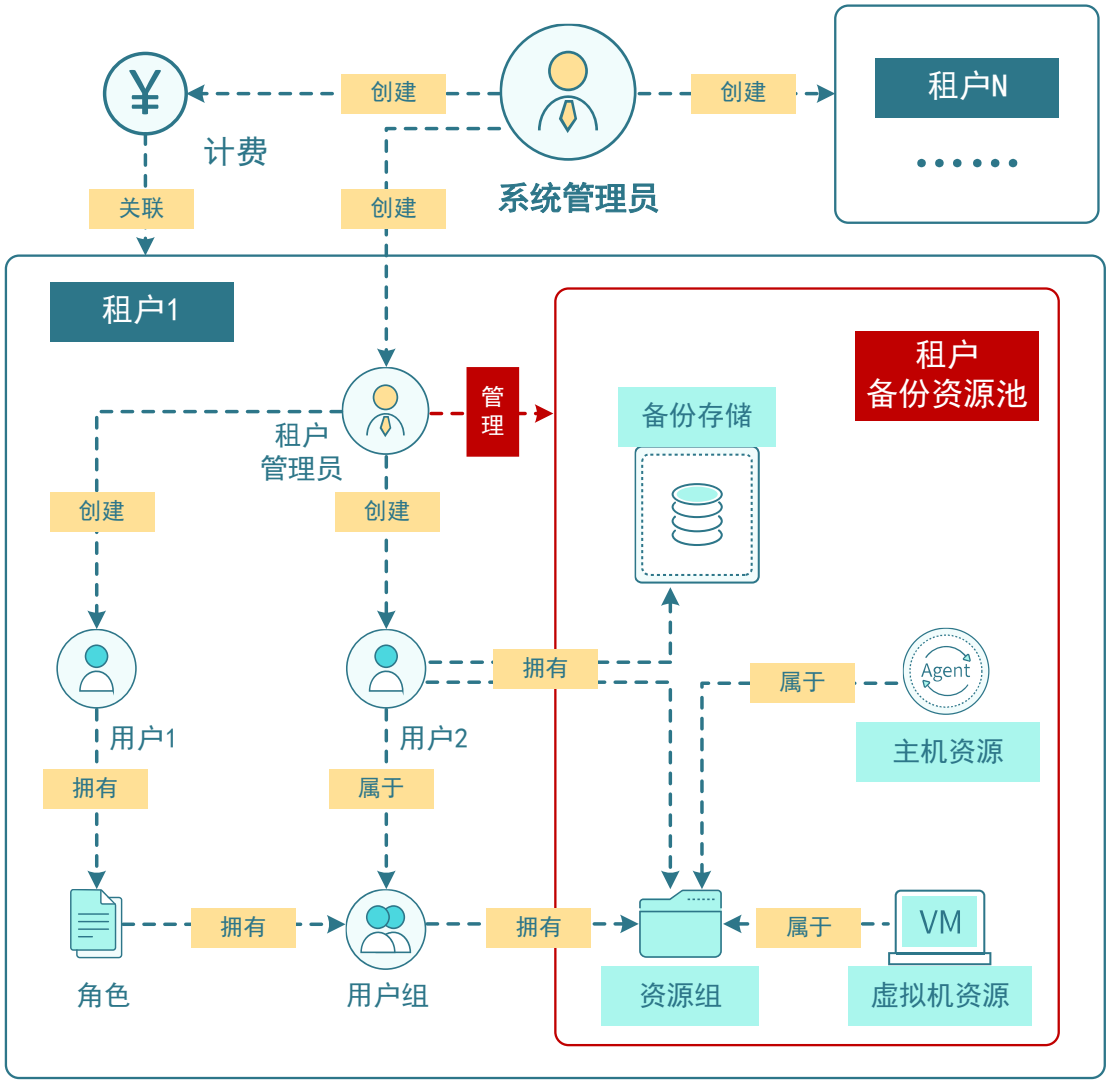


图 4-13 多租户逻辑关系

表 4-3为图 4-13中元素名词的解释说明。

表 4-3 多租户名词解释说明表

类别	说明
系统管理员	备份系统最高权限管理员
租户	相当于一个门户或组织架构的合集，一组用户、角色、资源的合集，除了系统管理员之外，内部信息和操作只有内部具有相应角色权限的用户可见
计费规则	用于记录一种系统计费规则，一个租户最多只可以跟一个计费规则关联
租户管理员/租户用户	租户内的用户，实际上图中租户管理员是拥有对应角色权限的用户，租户内用户可视范围被限定在指定租户中，关于用户相关和概念请参考章节 5.1
租户角色	租户内的一组权限集合，详细内容和概念请参考章节 5.1
租户用户组	拥有相同角色权限的多个用户的合集
资源	可分配给用户操作和使用的内容，在备份系统中主要资源包括生产虚拟机、代理、备份存储、资源等
资源组	多个资源的分组合集

4.3. 功能特点

- **配置多个租户、租户之间信息隔离，互不影响**：支持一个环境中配置多个租户，满足云环境中不同用户的资源分配和使用需求，同时能够有效屏蔽租户之间的信息，提高安全性；
- 可**配置灵活的计费功能**：支持创建计费策略，提供按时间或按量的计费方式，同时可以配置多个不同的计费规则，应用于不同的租户环境；
- **资源可分配，提高资源访问安全性**：租户内的资源可以根据一个组织架构的管理安全性进行分配，用户无法访问未分配的资源，无法恢复和访问他人产生的备份数据；
- **提供第三方或云 MSP 集成开发的 API**：系统提供标准的 REST API 接口，便于第三方或者 CMP 的集成开发，方便 MSP 给用户提供云环境的容灾备份服务；

5. 运维管理

5.1. 用户管理体系

为满足对系统管理操作和系统操作的安全需求，云祺容灾备份系统提供了高度灵活的用户管理体系，由角色、用户组及用户三者构成，具体说明见表 5-4。

表 5-4 用户管理体系组要组成元素说明

类别	说明
角色	一组权限的集合，其中权限包括操作权限和资源权限，决定了拥有该角色的用户能够看到什么和做什么。
用户组	一组用户的集合，通常情况下，该组下的用户具有一样的权限，用户组可以设置与多个角色关联
用户	容灾备份系统的基础，自然人操作和实用系统的主体，用户以名字作为主体标识。

用户、用户组及角色三者之间的关系如图 5-14所示。根据图中描述，可以知道，用户无论是直接亦或间接的，都必须要拥有一个角色，否则该用户无法执行任何操作，相当于无效的用户。同样的目前用户组必须至少拥有一个以上的角色权限。

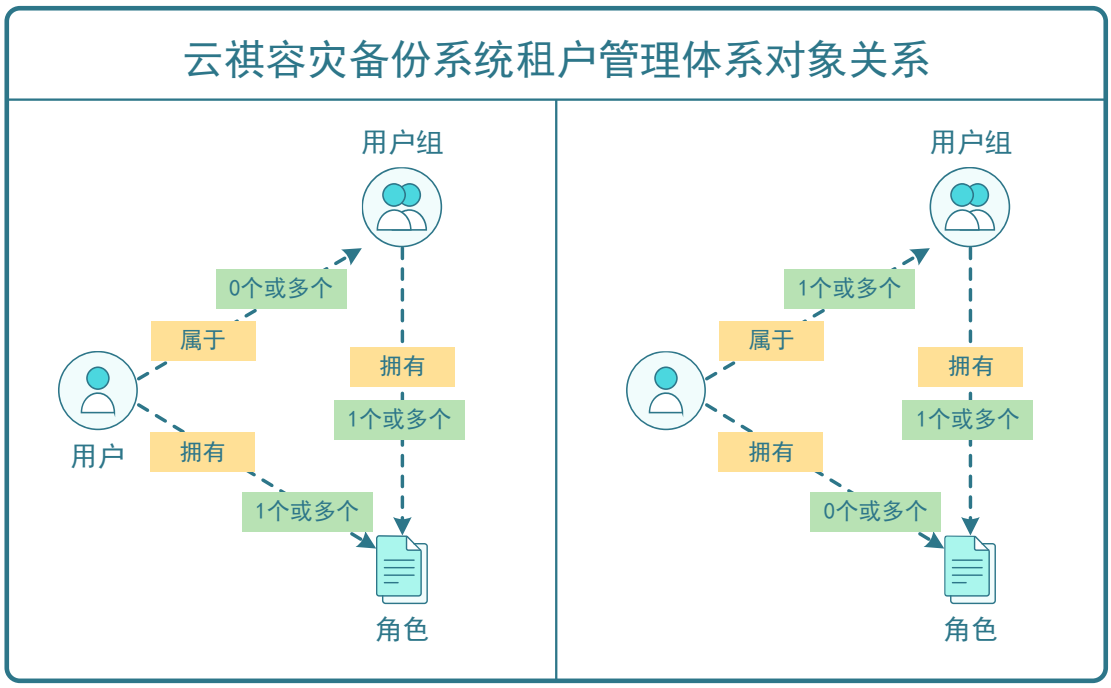


图 5-14 管理体系对象关系图

针对用户自身拥有角色，而其同时又在某一个或某几个用户组下的情况，其最终权限相当于所有权限的并集，例如用户U个人拥有A角色权限，用户U在某个用户组G，用户组G拥有角色B和角色C权限，则最终用户U的角色权限是A、B、C角色权限集合。

5.1.1. 角色及用户组说明

云祺容灾备份系统提供了预设的角色和用户组，默认的设置基本可以满足大部分用户的需求，具体的预设角色和用户组说明见表 5-5和表 5-6。

表 5-5角色配置说明

角色标识	角色名称	说明
Master	系统管理员	拥有系统所有资源和操作权限
Admin	管理员	系统监控，资源管理，系统管理，用户管理等
Operator	操作员	任务管理
Auditor	审计员	任务查看，告警、日志、报表等
Tenant Admin	租户管理员	租户内管理员权限
Tenant Operator	租户操作员	租户内操作员权限
Tenant Auditor	租户审计员	租户内审计员权限

表 5-6用户组说明

用户组标识	用户组名称	预分配角色权限
Master	系统管理员组	Master
Admin	管理员组	Admin
Operator	操作员组	Operator
Auditor	审计员组	Auditor

5.1.2. 角色关系

配置下的角色关系如图5-2所示，可以满足大部分用户的用户管理需求。

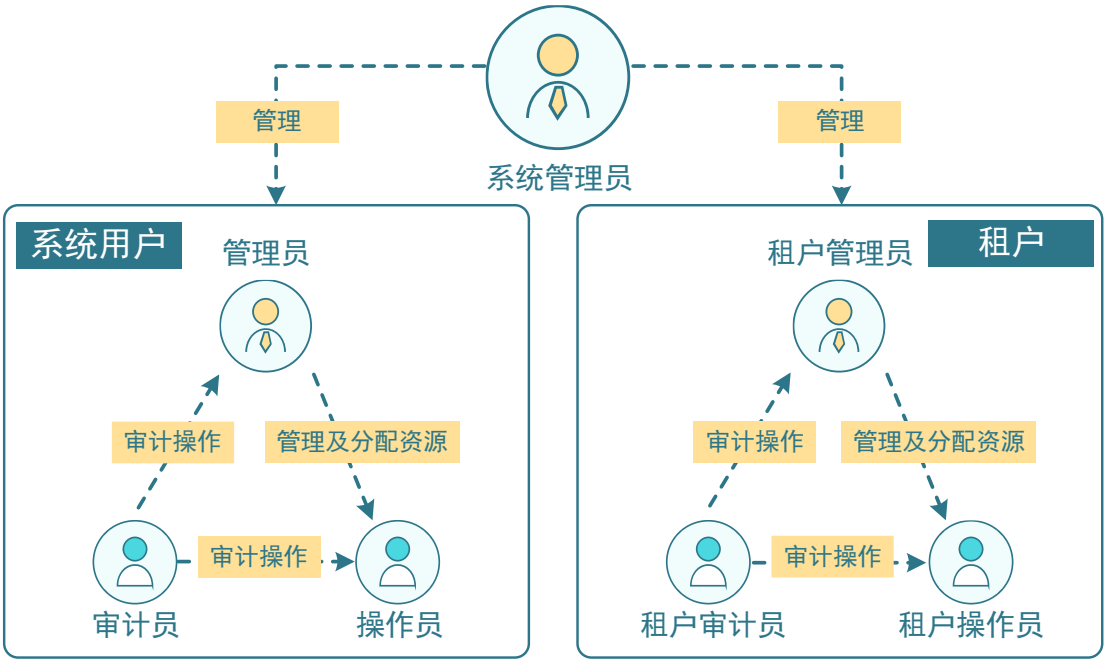


图 5-15 角色关系

由于系统本身支持灵活的角色权限配置，同时支持禁用/启用角色、用户组和用户的功能，因此可以通过设置，配置出更加安全和适合自身环境的角色权限。

5.2. 运行监控

5.2.1. 日志审计

系统提供两种类型的日志用于审计，分别为任务操作日志和系统操作日志，分别记录任务和系统相关联的操作信息，在任务或系统出现错误或异常的时候，可以根据日志进行追踪和回溯。下表为两类任务所包含的主要内容：

表 5-7 日志类别说明表

日志类型	说明	记录的信息
任务操作日志	该类型日志主要记录所有与任务相关的操作，包括所有类型任务的创建、删除、修改等	任务别名、模块类型、任务类型、任务操作关联用户、日志产生时间、日志
系统操作日志	该类型涵盖了系统内部除了任务相关所有操作的日志，如用户登录、系统配置、用户管理、资源管理等操作的日志。	用户名、操作时间、日志状态、操作信息描述

根据审计要求和不同日志反应的情况差异，将日志状态分成三种，分别为：

- **正常**：正常执行的任务或正常完成的系统操作
- **警告**：出现警告的任务或出现异常的系统操作
- **错误**：出现错误的任务或出现错误的系统操作

5.2.2. 统计报表

目前备份系统提供两种类型的报表用于数据统计，包括存储报表和虚拟机报表。报表采用图形和表格相结合的方式，以最直观的形式呈现给客户，所有报表均支持导出功能，方便用户进行日常的审计工作。以下针对每个类型的报表进行说明：

存储报表是对系统所有存储设备的统计报告，可以通过存储情况的使用情况，作为用户规划使用存储的依据。系统通过空间和时间两个维度统计备份存储的使用情况，详细说明见表 5-8。

表 5-8 存储报表展示维度说明

维度	说明
空间	以整个系统为视点，总体呈现系统内所有存储的用量，以及存储数量，在线/离线情况等；通过表格加图形的形式展示每个节点上存储的用量，存储关联任务数
时间	通过图标的形式展示某个时间范围内的总使用量和日均使用量，支持近一周到三个月的时间筛选

虚拟机报表是对系统保护虚拟化情况的统计。包括虚拟机备份状况统计和已备份虚拟机详情。统计分类说明见表表 5-9。

表 5-9 虚拟机报表统计分类说明表

分类	说明
虚拟机备份状况统计	以整个系统为视点，总体呈现系统内所有存储的用量，以及存储数量，在线/离线情况等；通过表格加图形的形式展示每个节点上存储的用量，存储关联任务数
已备份虚拟机详情	统计所有备份虚拟机情况，同时支持按单个虚拟机查看备份情况，统计虚拟机每日备份情况和最近一个时间段内的每日备份存储用量

5.2.3. 告警通知

系统提供两种类型的告警信息，分别为任务告警、系统告警。告警信息生成后可以通过邮件或短信的形式第一时间通知到管理员，方便管理员快速响应。

任务告警是系统所有任务运行的情况出现异常或错误产生的告警信息。包括了系统所有功能模块的任务。任务告警分成了两种等级：

- **警告**：任务运行中出现一些需要关注不影响任务正常完成或任务没有全部完成时候的告警信息。
- **错误**：任务中出现了错误，需要人工干预的任务。

系统告警是系统层面出现了异常或错误产生的告警信息。包括了系统整体运行情况、备份节点或存储情况、系统配置情况等。系统告警分成了三种等级：

- **一般**：系统运行中的一些提示性信息，可以不用特别关注。
- **警告**：系统运行中出现了异常，但是不影响系统整体运行。
- **错误**：系统运行中出现了错误，需要人工干预并处理。

5.3. 大屏展示

云祺数据可视化大屏展示，是将用户生产环境和数据保护系统的数据进行收集和整理，通过图形、图标、 图像、动画等一系列视觉元素，在数字化大屏幕上进行直观、多维、实时、动态等具有视觉冲击力的可视化展示。从用户角度，将核心数据外化于形，整合边缘数据，对数据进行深度剖析，再通过可视化大屏展示系统，帮助业务人员分析数据，发现、诊断业务问题，从而提升企业决策效率和工作效率。

通过大屏展示的信息包括：

- **系统概览**：图像化展示系统整体运行情况等信息。
- **节点监控**：包括备份节点的内存、CPU、网络流入流出、系统负载、磁盘 BPS、磁盘 IOPS 等信息。
- **存储统计**：所有存储数量和存储使用量，每个存储的使用情况等。
- **任务统计**：当前所有任务的整体统计情况，每个任务的运行情况等。
- **告警统计**：系统所有告警数量统计等。
- **模块信息统计**：按模块进行信息统计展示，包括虚拟机、文件、数据库、操作系统、实时备份、NAS 备份等。

5.4. 系统安全

5.4.1. 备份系统元数据备份

备份系统本身作为一个特殊的应用系统，自身也会存在着软硬件故障产生的风险。目前针对备份数据的安全性，云祺容灾备份系统可通过副本和归档功能进行多份存储，避免备份数据的单点故障风险。另一方面，云祺容灾备份系统提供了备份系统本身的元数据进行备份和还原的功能，故障发生后，可将备份出来的元数据恢复到新环境之中，而无需重新对备份系统进行配置。

其备份元数据对象如表5-7所示。

表 5-10 可备份的系统元数据对象表

编号	类别	元数据子项
1.	用户管理	用户、用户组、角色、域服务器
2.	基础设施	备份节点、备份存储、LAN-Free 配置、策略组、资源组
3.	多租户	租户、计费
4.	备份资源	虚拟化中心、客户端、传输代理
5.	任务	当前任务、历史任务
6.	告警	任务告警、系统告警
7.	任务	当前任务、历史任务

支持的备份和恢复模式如表5-8所示：

表 5-11 备份系统备份元数据对象表

编号	类别	方式	说明
1.	备份方式	按需备份	按需进行手动备份，备份后会通过浏览器将备份的元数据下载至本地
		自动备份	通过配置时间策略，将元数据自动备份到指定的备份存储； 支持配置按照个数保留的回收策略； 支持将已生成的备份点通过 WEB 进行下载；
2.	恢复方式	上传恢复	可通过将下载的备份文件通过 WEB 上传至修复后或新的备份系统上进行恢复
		通过备份存储备份时间点恢复	可通过备份存储内扫描出来的元数据备份点，选择指定时间进行恢复

5.4.2. 数据防篡改

近年来，网络安全形势已经变得越来越严峻，层出不穷的各种勒索病毒和黑客的攻击和入侵，对用户造成了巨大伤害和损失。容灾备份系统作为信息安全的最后一道防线，为用户提供了“后悔药”，但同样作为一个存储了大量数据的系统，如何避免勒索病毒和黑客对数据的攻击和篡改，也成为了用户和各大厂商关注的重点。

为了解决用户对备份数据遭到恶意篡改的顾虑，云祺容灾备份系统提供可配置的数据防篡改的功能。该功能可以有效的从系统层面阻断非白名单内的程序、人为非法数据访问和修改，可以有效保护容灾备份系统后台的服务文件、备份数据文件、内部数据库文件、依赖库以及配置文件等的完整性和正确性。

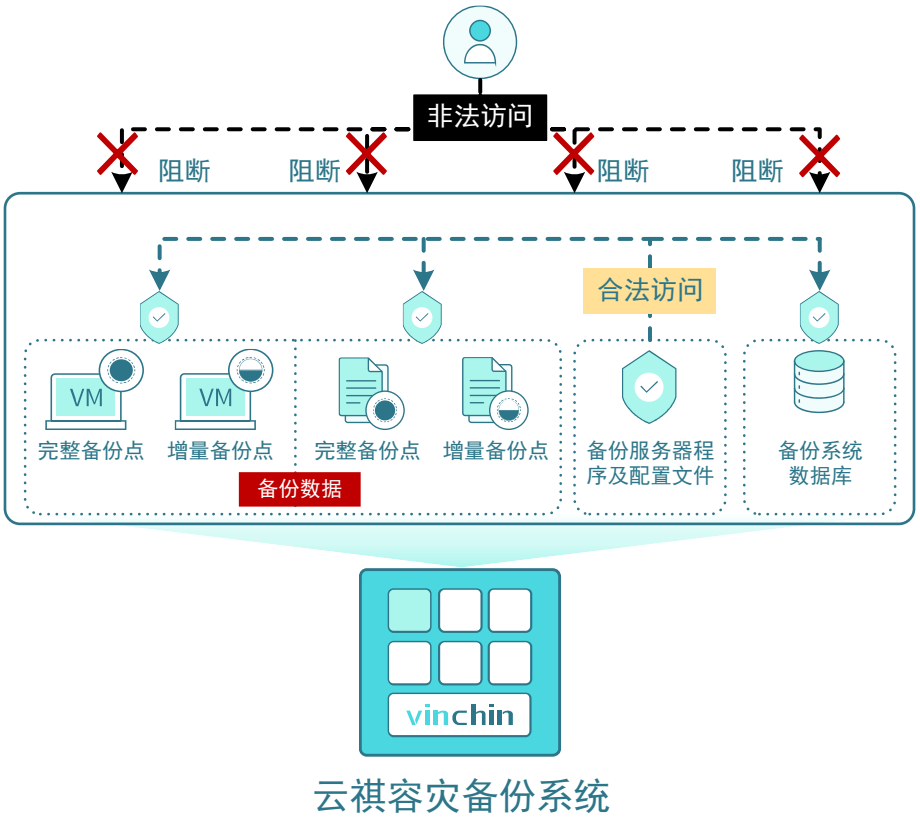


图 5-16 备份系统数据防篡改功能

vinchin

云 祺 科 技

热线：400-9955-698
邮箱：support@vinchin.com
电话：028-85530156
网站：www.vinchin.com
地址：中国（四川）成都云华路333号国家西部信息安全产业园8栋5层

欢迎关注
云祺官方公众号

欢迎咨询
云祺客服

欢迎关注
云祺官方视频号