爱数 AnyVault

www.eisoo.com/cn

EISOO 爱数
安 全 备 份 存 储

新一代远程数据灾备平台 - AnyVault

有价值的产品 有价值的服务 有价值的应用

爱数 AnyVault 平台

目录

概述

一、应对容灾，远程数据灾备服务化

■ 远程灾备，严峻的挑战

地震、水灾、火灾……天灾突如其来；错误操作、人为破坏、恐怖袭击……人祸防不胜防；设备失效、软件错误、通讯中断、病毒木马……技术风险无处不在。在企业越来越依赖信息系统安全运行的今天，一旦业务中断、数据丢失，可能造成的是致命威胁。而遭遇影响公司运营的意外情况也越来越普遍，数据显示，40% 的企业平均 3 年就会遇到一次意外威胁。

随着我国信息化的发展，组织越来越依赖信息技术，数据以指数方式增长，大量的数据在带给企业和组织巨额有形和无形财富时，数据的安全问题已日渐成为关注的焦点，特别是 2008 年我国南方发生的大面积雪灾、四川5.12大地震给国家和人民财产造成了巨大的损失，给灾后的恢复带来难以估量的困难，数据的容灾备份问题也再次引起各级组织的高度重视。

然而面对越来越重要、越来越复杂环境下的数据保护难题，容灾几近成为企业和组织面临的巨大挑战：

- ✧ **成本挑战**

  面对远程灾备中心的高昂成本，远程容灾成为大部分企业和组织可望而不可即的愿望；而传统的容灾模式是采用复杂的容灾系统和硬件，其专业性与复杂性是普通组织无法承担的 IT 负担。

- ✧ **一体化全面数据容灾挑战**

  数据不断增长，危机无处不在，企业将全面可靠的灾难恢复计划纳入到总体战略中尤为重要。这有助于确保灾难发生时，企业能成功地恢复数据和应用，最大限度减少对业务的影响。

  IDC 相关专家建议企业跨越虚拟环境、远程办公、桌面系统、笔记本、服务器、应用程序和数据库实施全面数据保护解决方案，这样可在发生灾难时迅速恢复关键数据和系统。

- ✧ **远程容灾带宽挑战**

  迅速发展的企业无一例外受到管理和存储不断增大的数据量的压力。大数据量的传送、存储和管理使传统的备份软件系统越来越难以满足要求。数据容灾战略需要能够便捷扩展以适应爆炸性的数据增长。

■ 灾备服务化，化解挑战的真正途径

专业化建设和社会化服务已成为发达国家信息安全和业务持续管理服务行业发展的主要特征。灾备服务化或者说外包数据灾备业务为企业广泛实施远程数据灾备提供了一条切实可行的道路。利用厂商、服务运营商合作建设的灾备平台，提供的专业数据灾备服务，来实现企业的远程数据灾备。

■ 一体化远程灾备平台，灾备服务化的利器

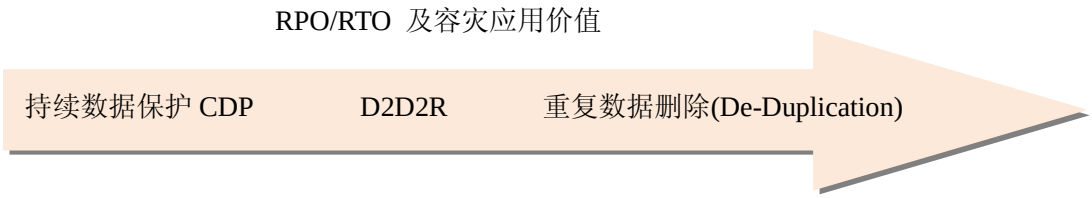
随着企业业务和应用的迅速增加，进行数据统一保护、远程容灾刻不容缓，一体化的远程灾备平台需要具有创新性、革命性等诸多特点：

1. 异构系统的一体化容灾特性：真实机与虚拟机；Windows、Linux、Unix 系统；服务器、远程办公、桌面系统、笔记本的统一容灾保护、整体方案管理；
2. 全面保护容灾特性：应用程序和数据库实施全面数据容灾保护，

3. 可运营平台：平台的规模化承载能力、可扩展性、安全性和容灾 RPO/RTO 目标必须是可运营的，同时平台的运营必须符合国家法规和条例。
4. 具有良好的管理性：为企业提供简易、可管理的平台，为运营提供安全、可靠、可监控的管理平台。

■ 突破平台瓶颈，应用决定价值

远程数据传输的瓶颈在于带宽，面对企业大量数据的容灾备份传输，容灾速度已经成为限制平台大规模实施和推广的桎梏。



无论是 CDP、D2D2R(Disk-to-Disk-Remote)或 De-Duplication 等任意一种备份模式与技术，对于容灾而言，其价值更多的在于其应用的模式：

1. 专家们一致看好持续数据保护 CDP 对于备份容灾的价值，它有效地提高了备份的 RPO/RTO；但是，RPO/RTO 的提升一定程度上意味着海量备份数据给网络带宽带来的的巨大压力，所以，一个适当的 RPO/RTO 对于远程容灾而言非常重要。
2. D2D2R 的应用价值在于双重容灾，本地脱机备份然后容灾到异地，极大的提高了备份的速度。
3. 将重复数据删除应用于远程数据灾备，除了节省存储空间，更重要的价值在于采用基于源端的重复数据删除，可以减少大量重复数据传输给网络带宽造成的压力，是大数据量异地容灾的最大价值所在。

平台建设篇

第一章 容灾与法规遵循

■ 容灾与备份，有法可依

2007 年 7 月，国务院信息化工作办公室领导编制的《重要信息系统灾难恢复指南》正式升级成为国家标准《信息系统灾难恢复规范》（以下简称“规范”）（GB/T 20988-2007 ）。这是中国灾难备份与恢复行业的第一个国家标准，已于 2007年 11 月 1 日开始正式实施。

《规范》中规定了信息系统灾难恢复应遵循的基本要求，适用于信息系统灾难恢复的规划、审批、实施和管理。《规范》具体对灾难恢复行业相应的术语和定义、灾难恢复概述（包括灾难恢复的工作范围、灾难恢复的组织机构、灾难恢复的规划管理、灾难恢复的外部协作、灾难恢复的审计和备案）、灾难恢复需求的确定（包括风险分析、业务影响分析、确定灾难恢复目标）、策略的制定（包括灾难恢复策略制定的要素、灾难恢复资源的获取方式、灾难恢复资源的要求）和策略的实现（包括灾难备份系统计数方案的实现、灾难备份中心的选择和建设、专业技术支持能力的实现、运行维护管理能力的实现、灾难恢复预案的实现）等内容作了具体描述。

根据该规范，我国信息系统灾难恢复分为 6 个等级，如下图所示：

第6级 数据零丢失和远程集群支持

- ✓ 完全数据备份至少每天一次；
- ✓ 实现远程数据实时备份，实现零丢失；
- ✓ 应用软件可以实现实时无缝切换；
- ✓ 远程集群系统的实时监控和自动切换能力；

第5级 实时数据传输及完整设备支持

- ✓ 完全数据备份至少每天一次；
- ✓ 实现远程数据复制技术
- ✓ 备用网络也具备自动或集中切换能力；

第4级 电子传输及完整设备支持

- ✓ 完全数据备份至少每天一次；
- ✓ 配置所需要的全部数据和通讯线路及网络设备，并处于就绪状态；
- ✓ 7*24 运行，更高的技术支持和运维管理

第3级 电子传输和部分设备支持

- ✓ 完全数据备份至少每天一次；
- ✓ 每天多次利用通信网络将关键数据定时批量传送至备用场地；
- ✓ 配备灾难恢复所需的部分数据处理设备；

第2级　备用场地支持

- ✓ 完全数据备份至少每周一次；
- ✓ 灾难发生时能在预定时间调配数据，通信线路和网络设备；
- ✓ 有备用场地管理制度；

第1级　基本支持

- ✓ 完全数据备份至少每周一次；
- ✓ 制定介质存取、验证和转储的管理制度；
- ✓ 完整测试和演练的灾难恢复计划；

图 1 信息系统灾难恢复等级划分

在我国的信息化发展过程中，信息系统的灾难恢复建设也逐步取得阶段性进展，但各个行业的发展不尽相同，如图 2 所示，相对而言，银行、金融业的容灾需求是最高也是最紧迫的，为了规范金融业灾备中心的建设，中国人民银行在 2005 年提出：全国各商业银行在 1～2 年内数据灾难备份标准达到 2～3 级，在各银行完成数据集中后的 2 年内灾难备份标准必须达到 5～6 级。

2006 年 8 月，证监会也发布了相关的安全指导，要求灾难备份中心对中心机房的数据备份等级要求应达到灾难恢复等级划分中的第 4-5 级。

紧跟银行、金融和证券等行业之后，政府、交通、通讯、电力、医疗卫生等行业也逐步进入规划建设阶段。

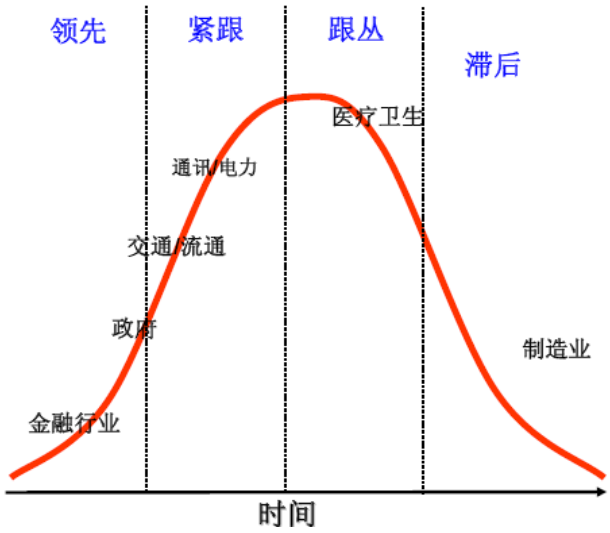


图 2 行业发展趋势

对于中国的绝大部分中小企业而言，受限于容灾等级的高额投入，在灾备方面的建设是比较滞后的。对于信息系统灾难恢复规范而言，备份系统的重要性显得非常重要，设计一个容灾备份系统，需要考虑多方面的因素，如备份/恢复数据量大小、应用数据中心和灾备数据中心之间的距离和数据传输方式、灾难发生时所要求的恢复速度、灾备中心的管理及投入资金等。

■ 信息等级保护，按需定位

对 IT 系统进行容灾，就容灾备份系统本身而言，也是整个 IT 系统的组成部分，其安全性规范是非常重要的。一个完整的容灾平台既包括了灾难恢复等级能力的满足，也包括整个容灾系统的安全保护体系规范的能力，根据

国家《计算机信息系统安全保护等级划分准则》(GB17859-1999) 的要求，对抗能力和恢复能力共同形成了信息系统的安全保护能力，以对抗不同的威胁和能够在不同的时间内恢复系统原有的状态。

根据 GB17859-1999 的规范，信息系统安全保护等级划分为五个等级，分别是：

- ✧ 第一级：用户自主保护级；
- ✧ 第二级：系统审计保护级；
- ✧ 第三级：安全标记保护级；
- ✧ 第四级：结构化保护级；
- ✧ 第五级：访问验证保护级。

对于不同的安全保护等级，能够在一定时间内恢复系统原有状态的能力构成了另一种安全保护能力——恢复能力。恢复能力主要从恢复时间和恢复程度上来衡量其不同级别。恢复时间越短、恢复程度越接近系统正常运行状态，表明恢复能力越高。

信息系统安全保护等级是信息系统灾难恢复规范的基础，而信息系统灾难恢复规范是信息系统安全保护等级的恢复能力的细化。大致上，对应信息系统安全保护的不同级别，其恢复能力是不同的灾难恢复等级。

综上所述 ,信息系统安全与容灾必须基于两个基本的国家标准规范(《计算机信息系统安全保护等级划分准则》GB17859-1999 和《信息系统灾难恢复规范》GB/T 20988-2007)，在此基础上，只有从底层基础平台建设、IT 基础设施、信息系统安全以及容灾备份系统的规范化建设，才能真正构建起符合国家标准的高安全、高可靠性和高可用性的信息系统和容灾系统。

第二章 平台建设分析

2.1 平台建设的系统分析

2.1.1 平台定义

远程数据灾备平台可提供灾备服务，以企业为基本单元，实现大规模并发、大数据量传输的企业级数据容灾服务。

平台通过网络传输，将用户端的数据传输到异地的数据中心备份起来，用户端一旦发生巨大自然灾害而导致数据损毁，可通过从异地数据中心将备份数据恢复出来，从而避免关键业务数据的彻底丢失。

2.1.2 平台建设的目标

与应用级和业务级灾备方案不同，远程数据灾备平台是满足第四级灾难恢复要求，属于数据级容灾范畴，并且具备向应用级和业务级容灾扩展的系统架构和基本能力。当灾难发生时，仅需要确保数据可在异地的数据中心完整的恢复出来。其灾难恢复计划也不需要像业务连续性灾备方案，能够迅速在灾备站点接管业务，而是以合理的 RTO 和 RPO 为基本目标。因此，远程数据灾备平台的建设相对于业务连续性灾备的建设，其复杂性、建设成本、管理和运营成本都相对较小，其建设目标应包括：

- **平台可用性**：包括 RTO 和 RPO、安全性、可靠性指标；
- **平台可运营性：**包括平台的适应能力、服务能力和扩展能力；
- **平台合规性：**包括在行业应用中法规遵从的要求；
- **平台风险可控性：**包括平台监控、数据和访问审计机制、报告机制和预先告警机制。

2.1.3 平台建设的关键技术指标

远程数据灾备平台因其基本的灾难恢复需求，面向多用户广泛应用并完全依赖于网络传输，所以其关键技术指标应包括：

- **RTO 和 RPO 目标：**RPO 指标必须小于 1 天，RTO 指标必须小于 16 分钟。
- **传输效率目标：**能够满足 TB 级数据量在广域网的传输要求。
- **可部署性目标：**用户接入平台进行数据采集时，能够完全适应用户现在环境，无论用户环境是运行在 FC-SAN 环境，还是 LAN 环境。
- **可扩展性目标：**服务器端须满足 PB 级数据量、上万服务器访问的吞吐能力和透明扩展能力。
- **安全性目标：**从用户接入数据采集到网络传输过程，到服务器备份数据保存须保证用户数据安全不泄漏。
- **兼容性目标：**需从 CPU 体系结构、操作系统、应用程序、网络结构、存储结构等多方面兼容用户环境。
- **合规性目标：**满足国家和行业法规标准中，对服务能力、恢复能力、保存方式和保存周期等法规的遵从。

2.1.4 平台的法规遵从约束

国家相关法规对远程数据灾备平台有着明确的约束：

- 平台所支持的信息系统灾难恢复等级规范约束；
- 在信息系统安全等级保护基本要求中，对恢复能力要求在遭到破坏后能够较快的恢复；

- ✧ 在计算机等级保护制度细则中，要求关键业务每天都必须执行完全备份一次；
- ✧ 在计算机等级保护制度细则中，要求备份数据既有近线保存，也需要离线保存；
- ✧ 要求为不同级别的业务数据提供不同级别的服务能力。

2.2 平台建设的系统架构分析

2.2.1 超越传统备份软件的架构

传统备份软件作为远程数据灾备平台建设时，面临着如下架构瓶颈：

- ✧ 传统的备份软件是面向单一企业使用的软件产品，当多企业同时使用时，面临着权限管理、数据安全、使用的可操作性等问题。
- ✧ 传统的备份软件在架构上不是为远程数据灾备而设计的，因此在远程传输稳定性、远程传输效率、远程传输安全、缓冲和传输加速等技术领域作了有限的设计。
- ✧ 传统的备份软件不具有可运营性，包括多用户使用的自服务能力、远程管理便利性，以及用户使用的业务结算。
- ✧ 传统的备份软件是面向有限变化的用户环境，面向多企业的灾备平台需要满足超大数据量和大批量机器的并发能力，以及能够实现按需部署，当新增加用户时，可透明的扩展介质、服务器，以满足新增的处理需求。

因此，在设计远程数据灾备平台时，必须从架构上重新设计，而不是采用备份软件在方案部署时克服局限性而强制的应用。

2.2.2 总体系统结构设计

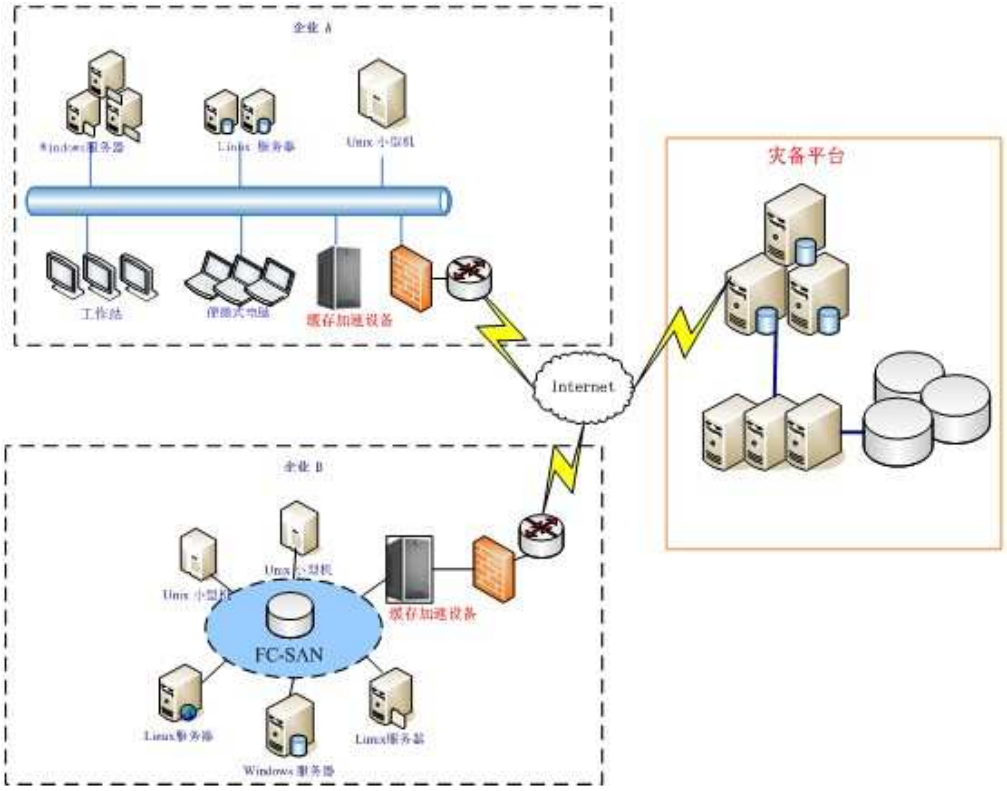


图 3 远程数据灾备平台的总体结构示意图

如上图所示，远程数据灾备平台的总体系统结构要求：

- ✧ 灾备平台可同时为多个企业同时提供服务能力，并且具有不同级别的服务响应性能。
- ✧ 灾备平台的服务器端应采用服务器和存储集群架构，划分不同职能角色向用户端提供高吞吐量和高可扩展的灾备能力。
- ✧ 灾备平台的数据传输网络可以采用 Internet 网络 ,Internet 网络作为当前通信和数据传输的基础网络，可保证灾备平台的建设具有可实施性和经济性。
- ✧ 灾备平台传输性能和传输优化是灾备平台可用的关键技术，总体系统架构中的缓存加速设备将扮演枢纽角色，可实现脱机备份和缓冲加速。
- ✧ 用户环境支持的广泛性，既可适用于服务器和工作站的灾备，又可满足 DAS、NAS、SAN 等存储结构的数据灾备需求。

2.2.3 以企业为管理单元的平台架构

远程数据灾备平台须满足多用户接入要求，其管理构架可采用以企业作为基本单元的总体设计：

- ✧ 每一个企业作为一个使用单元，从用户接入到数据采集到灾难恢复全程管理。
- ✧ 每一个企业可实现自服务，包括申请使用、权限管理、空间管理、备份计划管理、恢复管理、业务结算等。
- ✧ 在存储端，数据按企业为单位进行逻辑隔离，以确保不同企业数据的安全。
- ✧ 在服务器端，可基于企业为单位提供不同级别的服务能力，包括带宽使用量、存储吞吐能力和并发能力等，可基于企业为单位进行分级数据管理、离线归档和再容灾。

2.2.4 服务器端的平台架构

远程数据灾备平台的可用性、可运营性、合规性和风险可控性等目标的实现，最关键取决于灾备平台服务器端的平台架构，其架构必须满足：

- ✧ 服务器端须采用集群或群组架构，以提高系统的稳定性和吞吐能力，满足平台服务可靠性和可扩展性的目标。
- ✧ 服务器端的管理、维护和扩展对于用户完全透明，不需要停止服务和用户参与。
- ✧ 服务器端的系统部署须具有简单可实施特性，以免增加维护难度而降低平台的可用性。
- ✧ 服务器端集群和群组资源中，负载均衡算法可满足不同用户的服务级别要求，对于服务级别越高的用户，均衡算法分配的可用资源（网络、服务器处理能力、存储）越高。
- ✧ 服务器端的使用记录可满足平台风险可控性目标，包括详细的系统运行记录以用于审计、系统故障的预先告警。

2.3 平台建设的关键点分析

2.3.1 运营型的灾备平台

一个运营型的远程数据灾备平台应涵盖以下要素：

- ✧ **按需服务能力**：满足多企业的按空间、时间独立服务的能力，类似于 SaaS 模式，平台可以根据企业的数据备份空间大小、服务的时间提供服务，并且可以根据实际的需求更新服务时间或者调整备份空间。
- ✧ **透明扩展能力**：服务平台具有良好的可扩展性，包括服务平台存储空间的可扩展性、服务器处理能力

的可扩展性；随着企业数据量的增长而透明的增加平台存储介质，并能根据平台服务器的负荷能力动态的增加服务器来提高平台的处理能力。

- ✧ **服务结算能力**：作为可运营的平台，服务支付与结算能力是一个为企业客户提供自服务的主要接口，用户可以通过平台购买和结算相应的服务授权来获得相应的服务。

2.3.2 技术方案的承载能力

在建设远程数据灾备平台技术方案选项时，需要考虑技术方案的如下承载能力：

- ✧ **服务器端存储能力：**可以大致根据服务的规模来进行核算，如果每企业的数据量在 10TB，则 10000 企业的服务器端存储在 100PB 左右（考虑了压缩、安全冗余等条件下的存储），但是平台的存储部署能力肯定不会是一次性投入，而是根据业务的增长逐步增长的，所以，要求服务器端的存储能力能够根据需求逐步的无缝扩展。
- ✧ **服务器端数据吞吐量：**灾备业务是以数据流为主的网络应用，所以对于服务器平台的 I/O 吞吐量非常重要.
- ✧ **客户端并发量：**平台是否满足高并发的客户端处理能力，考虑到整个平台为众多企业客户提供共享式安全备份容灾服务，如果每企业的服务器客户端在 50-100，则 10000 家企业的客户端数超过 50 万，并发概率在 0.1～0.15 之间，则并发处理能力必须超过 10 万。
- ✧ **传输效率：**针对容灾等级 4 级的备份要求，每天进行数据的完全备份，在带宽有限的情况下，每天进行 TB 级的数据传输，基本是无法完成的，在网络传输协议进行优化的同时，也必须采用合成备份、重复数据删除等先进的技术解决方案来满足这种大数据量传输的需求。
- ✧ **关键业务系统准实时 RPO 目标：**根据容灾等级 4 级的需求，有必要对企业的关键业务系统实现准实时甚至实时的备份与恢复目标（ RPO < 16 分钟），在远程容灾平台上实现实时备份，一方面是 CDP 的技术，另一方面是如何可以保证持续性的数据传输的快速性和稳定性，甚至来说，怎样减少对生产系统的影响。可以考虑采用 D2D2R 先实现脱机备份，然后进行远程容灾。

2.3.3 平台安全性

在《信息系统安全等级保护基本要求》中，平台的安全应包括：

- ✧ **物理安全：**物理安全主要涉及的方面包括环境安全（防火、防水、防雷击等）设备和介质的防盗窃防破坏等方面。
- ✧ **网络安全：**网络安全主要关注的方面包括：网络结构、网络边界以及网络设备自身安全等，具体的控制点包括：结构安全、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范、网络设备防护等七个控制点。
- ✧ **主机安全：**主机系统安全涉及的控制点包括：身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、入侵防范、恶意代码防范和资源控制等九个控制点。
- ✧ **应用安全：**应用安全主要涉及的安全控制点包括：身份鉴别、安全标记、访问控制、可信路径、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制等十一个控制点。
- ✧ **数据安全：**保证数据安全和备份恢复主要从数据完整性、数据保密性、备份和恢复等三个控制点考虑。

2.3.4 平台适应性

整个平台的建设应该包括：

- ✧ 用户环境的可接入性：用户环境能否连接到平台中。
- ✧ 用户环境的兼容性：平台是否完全兼容用户已有系统环境，诸如各种平台的操作系统、应用程序等。
- ✧ 网络环境的适应性：平台是否可适应常用网络，不需要建设专用网络。
- ✧ 使用者的适应性：平台能否具有可操作性，保证大量不同单位的企业可以快速掌握并使用。

第三章 AnyVault—超越传统备份软件

AnyVault 是新一代远程数据灾备平台，它不仅仅是一款备份软件，而是一个远程数据备份容灾平台。无论是 Windows 平台还是 Linux 或 Unix 平台，是服务器还是桌面电脑，是企业自有机房还是大型运营性质的数据中心，是真实环境还是虚拟环境，是各类企业级数据库系统还是普通的文件数据，AnyVault 灾备平台都可以提供全面、持续的容灾保护，同时满足集中管理和高效异地备份需求，更以其高可靠性、高性能和易用性，成为众多企业级客户进行异地数据容灾的首选平台。

■ 一体化容灾平台，拥抱灾备服务

AnyVault 是一体化的灾备平台，面向企业提供远程数据灾备服务，它以企业为基本管理单元，既可以为大企业提供总部分支机构的整体容灾备份解决方案，提供行业容灾解决方案，也可以为地方运营商提供灾备服务平台建设，为区域内企业提供灾备服务。

AnyVault 平台具有丰富的应用支持能力，包括 Windows、Linux、Unix 在内的主流系统、32/64位异构硬件、真实机和虚拟环境的支持，支持各种企业应用数据库系统的热备与异机恢复，支持各种异构网络环境的统一容灾备份。

■ D2D2R，双重容灾，更快更安全的保护

基于 AnyCache 的 D2D2R（Disk-to-Disk-to-Remote）容灾，是 AnyVault 的高级容灾模式之一：

1. 对生产系统通过高速缓冲服务器进行高速离线备份，减轻对生产系统的影响；
2. 通过透明的异地同步，加速从本地到远程的容灾。轻松实现近线备份＋远程容灾的双重保险；
3. 可以加速灾难恢复演习和局部灾难恢复时，远程数据恢复的速度；
4. 基于 GVFS（Global Virtual File System）全局灾备视图的透明管理，真正的高级应用价值功能，简单易用产品形态。

■ 重复数据删除，远程数据容灾的高速路

AnyVault 平台采用基于源端的重复数据删除技术（De-Duplicate）,高达300：1的压缩比，获益的不仅仅是节省了巨大的平台存储空间，更加可贵的是基于平台全局的重复识别算法，源端的重复数据不再成为备份与恢复传输的压力。

■ 持续数据保护，更高 RPO/RTO 目标

CDP 技术侧重点不仅仅是在于备份，更重要的一点是瞬间恢复，CDP 的无缝恢复技术能够实现一定业务连续性指标。CDP 技术能够确定 RPO/RTO 指标，可按照用户要求，恢复到指定时间点。能够为各种类型的企业，提供不同类型的数据保护机制和系统保护机制。

■ 虚拟介质池，拥抱磁盘免介质管理新时代

备份介质管理作为所有备份系统的基本内容之一，一直因为其专业性、复杂性、难以扩展而饱受诟病。AnyVault 平台基于虚拟介质池 VMP 的服务平台存储管理，让介质管理真正的透明化，免除了介质管理的复杂性，可轻松实现容灾平台存储的无缝扩展。另一方面，节约 31% 的容灾管理时间，极大的减轻了企业管理员和操作者的介质相关管理复杂度。

第四章 基于 AnyVault 的远程数据灾备平台

4.1 AnyVault 系统总体架构

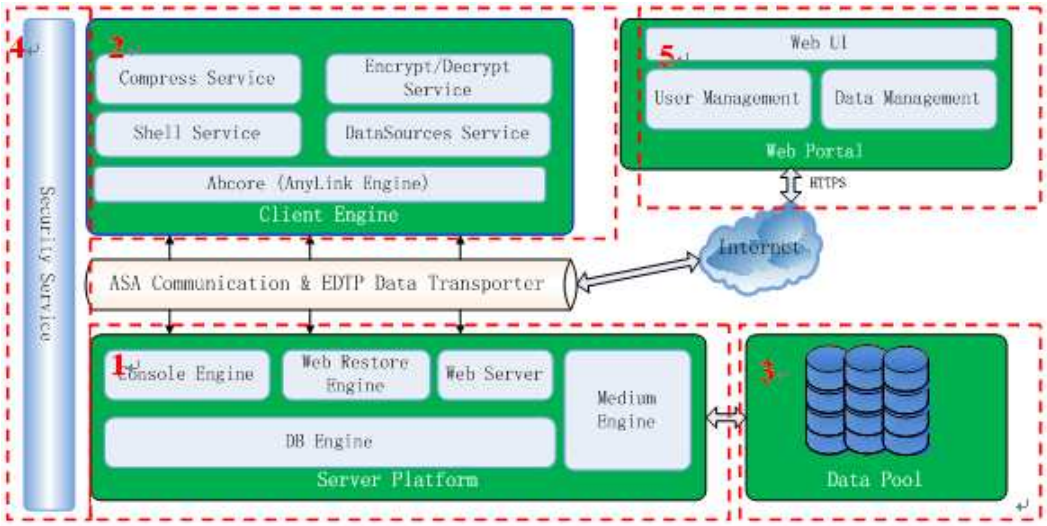


图 4 系统总体架构图

AnyVault 远程容灾平台包括数据源处理、压缩、加密、用户认证、通信、备份、恢复、存储，各个环节紧密协作，是一个完善的远程数据灾备平台。

如上图所示，该架构包含 4 个部分：

1. AnyVault 服务器平台端，如图所示第 1 部分；
2. AnyVault 客户端，如图所示第 2 部分；
3. AnyVault 服务器平台存储介质池，如图所示第 3 部分；
4. AnyVault 安全服务，如图所示第 4 部分；
5. AnyVault WEB 服务入口端，如图所示第 5 部分。

如上图所示，AnyVault 远程数据灾备平台的基本原理为：

- ✧ 灾备平台划分为服务器端和客户端，通过 Internet 网络传输，将用户端的数据传输到异地数据中心进行备份保存，用户端一旦发生巨大自然灾害而导致数据损毁，可通过从异地数据中心将备份数据恢复出来，从而避免关键业务数据的彻底丢失。
- ✧ 灾备平台可同时为多个企业同时提供服务能力，并且具有不同级别的服务响应性能。
- ✧ 灾备平台的服务器端应采用服务器和存储集群架构，划分不同职能角色向用户端提供高吞吐量和高可扩展的灾备能力。
- ✧ 灾备平台的数据传输网络采用 Internet 网络，为了保证大数据量容灾备份的可用性，系统采用重复数据删除、SmartMove 合成备份、D2D2R 缓冲同步容灾等关键技术来实现高可用性。

4.2 AnyVault 的系统目标

AnyVault 平台为企业提供灾备服务，以企业为基本单元，实现大规模并发、大数据量传输的企业级数据容灾服务，是新一代的远程数据灾备平台。其系统目标包括：

- ✧ **RTO 和 RPO 目标**： RPO < 1 天， RTO < 16 分钟。
- ✧ **传输效率目标**：能满足 TB 级数据量在广域网的传输要求。

- ✧ **可部署性目标**：用户接入平台进行数据采集时，能完全适应用户现在环境，无论用户环境是运行在 FC-SAN 环境，还是 LAN 环境。
- ✧ **可扩展性目标：**服务器端须满足 PB 级数据量、上万服务器访问的吞吐能力和透明扩展能力。
- ✧ **安全性目标：**整个系统基于 Double-Security 安全加密体系，网络传输过程采用标准 SSL 协议对通信过程进行加密、备份数据采用 AES256 进行加密；访问控制多认证模式，支持基于口令的访问控制、基于 USB-Key 的强认证访问控制以及混合访问认证模式。
- ✧ **兼容性目标：**在系统方面，兼容 Windows、Linux、Unix（IBM AIX、Sun Solaris、HP UNIX 等）等操作系统、支持 32/64 位硬件结构的备份与恢复；对于应用系统，支持 SQL Server、Oracle、DB2、Exchange Server、Lotus Domino、Sybase、Active Directory、SAP、SharePoint、MySQL、Postgre 等应用系统的容灾备份。
- ✧ **合规性目标：**平台建设完成，可以满足国家标准《信息系统灾难恢复规范》（GB/T 20988-2007）的 4 级容灾保护等级，平台本身满足《计算机信息系统安全保护等级划分准则》GB17859-1999 的第 4 级保护等级的规范。

4.3 AnyVault 关键能力初识

AnyVault 灾备平台具有六大特性：

1. **高性能并发平台**：满足大数据量、大并发客户端容灾备份的百万级并发平台，基于 AnyCluster 服务器集群模式的服务器端平台保证了整个平台的高性能、大并发的特性。
2. **离线备份+远程容灾的先行者**：基于 D2D2R 的容灾模式，一方面对生产系统基于缓冲服务器的高速离线备份，减轻对生产系统的影响，也可以加速服务器数据恢复的速度，另一方面，基于 GVFS 全局灾备视图的透明管理，可轻松实现本地备份+远程容灾的双重保险。
3. **重复数据删除**：高达 50 比 1 至 300 比 1 的压缩比，既可以大幅度减少数据中心存储的空间，更重要的是，基于全局的重复数据识别，极大的减轻了远程数据传输的压力。
4. **基于企业上下文的管理**：更加简单易用的平台，轻松实现容灾平台的服务化，企业 IT 管理员可以轻松的实现对企业内数据的容灾和保护。
5. **广泛而又全面的应用支持能力**：从文件、邮件到企业级应用数据库，可以全面保护企业的 IT 数据。
6. **免介质管理时代的领航者**： AnyVault 平台基于虚拟介质池 VMP 的服务平台存储管理，让介质管理真正的透明化，免除了介质管理的复杂性，可以轻松实现容灾平台存储的无缝扩展。

第五章 AnyVault 关键指标

5.1 RTO 和 RPO 目标

关于灾备的 RPO 和 RTO，RPO 是对备份时的时间连续性间隔长度目标，而 RTO 则是对灾难恢复是的时间长度目标。

对于 AnyVault 平台的恢复点目标 RPO，在平台的客户端采用基于 VSS 和文件系统监控的 CDP 技术，可以保证连续性的备份变动的数据。另一方面，为了减少连续性 RPO 目标对远程传输的压力，在客户端监控目标到远程灾备中心，AnyVault 的缓冲服务器起到了很好的桥接作用，经实践证明，在持续数据保护应用到远程数据容灾的场合下，D2D2R 更能保证系统的 RPO 目标。

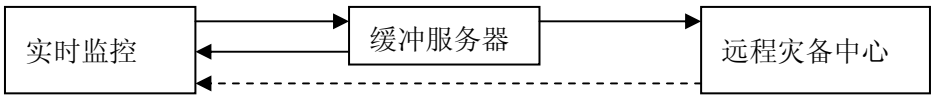


图 5 基于缓冲服务器的备份与恢复示意图

对于 RTO，当发生灾难事件时，如果仅仅是服务器硬件或者系统崩溃，那么，基于缓冲服务器的恢复，能够在很短的时间内（远远少于远程恢复的时间）恢复系统。而如果是较大的灾难，没有缓冲服务器的情况下，用户也能够从灾备端恢复数据在设定的数据量和带宽情况下数据恢复数据时间，以及恢复数据的有效性保证，满足恢复到客户端或者通过 WEB 恢复然后下载恢复压缩数据包。

5.2 传输效率目标

备份空间的占用情况表现：能够节省足够的备份空间满足采用合成备份算法，在服务器端定期进行完全备份合成或者增量备份合成，压缩备份空间。

AnyVault 平台在带宽有限的情况下，为了满足高速的传输目标，主要在两个方面进行了优化：

1. 传输优化 :AnyVault 平台对 EDTP 传输协议进行优化 ,满足在远程网络数据传输时最大化的利用带宽。该协议专门用于备份和恢复数据的传输优化，特别是广域网高延迟网络。其关键算法是采用异步多路分帧技术，在广域网高延迟网络环境中，网络带宽使用率高达 90% 以上。
2. 系统优化：包括两方面优化，首先，在服务器端采用合成备份节省备份的数据量，缩短备份窗口，减小客户端压力和网络资源占用；另一方面，采用基于源端的重复数据删除技术，大大减少重复数据的网络传输。

5.3 可扩展性目标

可扩展性须从简单扩展升级到透明扩展。

- ✧ 用户端系统接入扩展容易 :AnyVault 平台采用基于企业管理单元 ,企业管理员可以添加相关的普通用户、客户端进行管理，企业可以轻松的完成对所有需要保护的生产系统的服务器和 PC 的备份与恢复，具有良好的可接入扩展性。
- ✧ 灾备端用户扩展容易：一方面平台管理员可以添加相关的企业单元进行管理；另一方面，企业管理员可以轻松的添加相应的普通用户。
- ✧ 灾备端备份空间扩展容易：AnyVault 平台基于虚拟介质池 VMP 设计，可轻松实现存储空间的扩展，平台介质具有很好的弹性扩展能力。

- ✧ 灾备端备份系统扩展容易：应用服务器（引擎服务器、恢复服务器）采用集群和群组模式，可以根据企业和客户端的规模轻松扩展。

5.4 安全性目标

AnyVault 平台的安全性主要基于四个方面：

1. Double-Security 级数据加密：数据备份打包和存储时支持 AES、Blowfish 等多种高强度加密，并且在传输过程中 EDTP 协议可支持 SSL 安全套接字，在网络链接传输时经过多重加密从而保证备份和恢复的安全可靠
2. 强身份认证：AnyVault 可支持 USB-Key、数字证书等强身份认证方式。有效克服密码安全性低、不易使用、效率低下等缺点，为企事业单位为用户访问内部和网络数据提供安全可靠的方法。
3. 基于公钥密码技术的 CA 认证：AnyVault 平台根据身份令牌中的用户信息和公钥生成 CA 数字签名，进行身份认证以及备份密钥加密传输。
4. 企业上下文（Enterprise Context）：在 AnyVault 灾备平台中，引擎服务器、介质服务器等都运行在虚拟的企业上下文环境，每一个企业上下文都包含权限信息、使用元数据，用户令牌信息等，不同企业的上下文环境采用逻辑隔离，以保证每一个企业的安全性都完全独立，不会受到关联性影响。

5.5 AnyVault 平台的应用关键指标

AnyVault 远程数据灾备平台可支持的平台和应用清单如下：

项目	*内容*
CPU 体系结构	*x86、x64、IA64、SPARC、Ultra SPARC、PA-RISC、PowerPC*
操作系统	*Windows、Linux、AIX、Solaris、HP-UX*
虚拟化平台	*VMware Virtual Infrastructures、Windows Hyper-V、Xen*
数据库	*SQL Server、Oracle、Sybase、Exchange Server、Lotus Domino、DB2、Active Directory*

第六章 AnyVault 平台建设规划

6.1 服务器平台的建设

6.1.1 建设指标

远程数据灾备平台的建设指标主要包括：

1. 灾备平台服务规模指标
2. 与服务规模相对应的服务器投入指标
3. 与服务规模相对应的存储指标

其中服务规模指标主要是平台面向的客户群体规模，主要相关参数包括：

1. 企业数；
2. 企业服务器、客户端数；
3. 企业数据容灾规模（数据量）。

假设平台服务的企业数为 2000，每个企业需要包含的服务器和 PC 平均 20-50 台，每机器备份的数据量在 50GB，那么总的数据量 5PB 左右。

6.1.2 服务器建设规划

爱数 AnyVault 服务器平台在逻辑上由五部分组成：

1. 引擎服务器
2. 介质服务器
3. 恢复服务器
4. 数据库服务器
5. WEB 服务器

其中，引擎服务器、介质服务器采用群组模式进行扩展，而恢复服务器、数据库服务器和 WEB 服务器可以采用集群模式进行扩展。各种服务器的要求如下：

1. 引擎服务器是整个服务器平台的核心部分，负责企业内的客户端、缓冲服务器等 Agent 服务的连接，基于客户端 Agent 服务连接的各种调度。因为它基于相应企业上下文（Enterprise Context）操作，所以采用群组模式(Group)，企业单元(相应的客户端 Agent 及相关的操作)与相应的引擎服务器绑定。服务器规模根据每服务器 2000 客户端并发规划建设（并发概率在 0.1-0.2 之间）。
2. 恢复服务器负责 WEB 恢复的请求，与企业上下文无关，可以进行集群，建设规模根据每服务器 2000 客户端并发规划建设（并发概率在 0.1-0.2 之间）。
3. 介质服务器负责读取或者写入备份数据，负责管理真实介质。介质服务器既可以采用集群，也可以采用群组模式，建设规模根据每服务器 2000 客户端并发规划建设（并发概率在 0.1-0.2 之间）。
4. WEB 服务器是整个服务平台采用 B/S 架构，基于 Web 的操作模式，是系统的入口。建设规模根据服务器负载的增长而进行集群扩展（基于 DNS 负载均衡）。
5. 数据库服务器是平台的信息持久层。采用 M-M 数据库集群配置模式，根据每服务器 2000 客户端并发的规模进行建设。

综上所述，对于 20000 客户端（0.2 并发概率）为标准的建设为基础，其服务器的标准配置为：

表 2.　2 万客户端服务器平台标准配置

服务器名称	*服务器数量*	*标准配置*
引擎服务器	*2*	*CPU PD 或者至强，内存 4GB 以上，*
恢复服务器	*2*	*CPU PD 或者至强，内存 4GB 以上，磁盘空间 500GB 以上*
WEB 服务器	*2*	*CPU PD 或者至强，内存 4GB 以上*
介质服务器	*2*	*CPU PD 或者至强，内存 4GB 以上，磁盘空间 1TB 以上（建议使用 NAS 设备）*
数据库服务器	*2*	*CPU PD 或者至强，内存 4GB 以上*

6.1.3 存储建设规划

容灾备份平台目标存储设备可支持各种架构的存储设备，空间利用率高，介质存储池既可以是 SAN/NAS/IP-SAN 也可以是集群存储系统。

根据服务规模，可以随时扩展。比如基础的 20000 客户端备份，每机器的数据量在 50GB，那么，总的数据容量在 1PB。

另外，为了保证存储的安全性，有必要采用存储的冗余建设，如果存储采用集群存储系统，比如 Lustre 集群文件系统，那么，冗余安全性可以由集群存储系统可以很好的保证，如果采用 SAN/NAS 等，则需要进行服务器存储的容灾。容灾模式可以是异地同步模式，备份的数据然后同步到额外的存储设备。那么在上述的情况下，需要 2PB 的理论存储容量。

在 AnyVault 平台中，采用了重复数据删除，对于实际而言，1PB 的需求，实际压缩比在 80 倍左右，则实际的存储容量 15TB 左右，所以总存储容量实际是 30TB 左右。所以，在平台化的重复数据删除技术下，可以极大的节约存储空间。

6.2 服务器平台网络带宽规划

因为远程数据容灾是一种以数据传输为主的网络应用，所以对于网络带宽而言是整个应用的关键之一。

在整个 AnyVault 平台中，每个服务器承担的责任不同，相对而言，介质服务器是数据备份与恢复的接口，所以他们的带宽是平台的瓶颈所在。我们根据每服务器 2000 并发来计算，每客户端的平均为 200KB/s，那么每服务器的带宽需要 200MB/s (约 2Gbps 带宽)。

在这种情况下，服务器平台面临两个问题：

1. 如何解决窄带的传输问题：在 AnyVault 平台中，主要采用重复数据删除技术来解决大数据量重复传输的问题。另一方面，服务器端合成备份也是系统的关键技术之一。
2. 如何提供基于服务质量的服务：在 AnyVault 平台中，可以为每个不同的企业提供个性化的网络定制化服务，保证其在服务器端传输网络的足够带宽保证。

6.3 AnyVault 平台部署场景应用

6.3.1 服务器端部署

AnyVault 平台服务器端部署主要是指 5 大服务器的部署，主要包括：

1. 基本服务器部署：基于 Linux RedHat Enterprise4 服务器平台。
2. 服务器集群部署：恢复服务器基于 LVS 集群模式，需要增加 LVS Director 服务器的部署和相关配置。
3. 服务器群组部署：引擎服务器和介质服务器，只需要进行平台相关的配置即可；

4. WEB 服务器集群可以采用基于 DNS 负载均衡的集群模式。
5. 数据库服务器采用 M-M 模式配置集群。

6.3.2 网络部署

服务器平台的网络分为两部分，服务器内部千兆局域网和对外接口网络。

1. 5 大服务器内部采用千兆局域网部署，保证服务器通信的速度；
2. WEB 服务器、介质服务器、引擎服务器需要有对外的网络连接，接受客户端的访问。

6.3.3 用户接入部署

在 AnyVault 平台上，用户端的接入比较简单，主要步骤包括：

1. 平台管理员为企业开通相关服务；
2. 在需要备份和保护的客户端（服务器或者 PC）安装 AnyVault 客户端软件（包括 Windows、Linux、Unix 客户端）。
3. 管理员或者相应的用户为客户端创建相应的备份任务，并设定相应的备份计划，或者启动实时备份。

6.3.4 缓冲服务器部署

在 AnyVault 平台上，可以采用缓冲服务器实现 D2D2R 异地容灾方案，其优势有：

1. 轻松获得本地和远程双重数据保护效果；
2. 离线备份+远程容灾，对生产系统的影响更小。

部署缓冲服务器的企业，可以采用专用的缓冲服务器或者在已有的服务器上安装相应的缓冲服务器服务。并指向响应的容灾中心服务器即可。

6.3.5 数据灾难恢复计划

灾难恢复计划是一个全面的状态，它包括在事前，事中，和灾难对信息系统资源造成重大损失后所采取的行动。灾难恢复计划是对于紧急事件的应对过程。在中断的情况下提供后备的操作，在事后处理恢复和抢救工作。

数据的灾难恢复计划主要包括以下几个部分：

1. 数据连续备份计划：针对企业可以容忍的数据灾难程度建立备份计划。
2. 数据恢复计划：针对保持数据恢复的有效性和时效性，建立灾难恢复制度；
3. 灾难恢复演习计划：针对企业制定灾难恢复演习计划，定期针对系统进行相关系统数据的灾难恢复演习。
4. 以上计划均应参照相关国家法规和行业法规进行。

第七章 AnyVault 服务价值

7.1 平台的总体拥有价值 TVO (Total Value of Ownership)

总体拥有价值 TVO 是针对项目的投入和价值产出比而言的。AnyVault 远程数据灾备平台能够给用户带来最大的总体拥有价值。

对于企业客户而言，IT 信息数据作为企业的核心资产之一，对数据的容灾和保护，本身是一项持续性的投资，投资的总体成本 TCO 包括灾备中心建设成本、硬件、软件平台、维护成本和人力成本投入：

$$TCO = 灾备中心建设成本 + 硬件成本 + 软件平台 + 维护成本 + 人力成本$$

而采用 AnyVault 容灾平台提供的企业异地数据灾备服务，企业的 TCO 变为：

$$TCO' = 灾备服务成本 + 维护成本' + 人力成本'$$

对于采用 AnyVault 灾备平台企业而言，其维护成本和人力成本已经不再等同与自建容灾中心的投入了，通过专业的灾备服务，其维护成本仅限于企业信息中心 IT 人员对内部网络数据备份环境的维护，实际上，采用 AnyVault 灾备平台提供的服务，对于企业而言，其总体拥有成本 TCO 已经达到最小化。

容灾价值(Disaster Recovery Value)在于发生灾难时对数据的及时恢复，通常我们通过数据单位价值成本、数据量、灾难发生概率、灾难恢复时间成本的综合来获得容灾价值。

$$DRV = (每MB数据成本 \times 数据量 + 灾难恢复时间成本) \times 灾难发生概率$$

这样，可以获得 TVO 的计算公式：

$$TVO = \frac{DRV}{TCO'}$$

对于企业客户而言，由于采用灾备服务的总体拥有成本 TCO 已经最小化，这样，一定企业的容灾价值与 TCO 比例就获得了最大化。

7.2 平台的可操作性

远程数据灾备平台以满足多用户接入使用为功能目标，因此良好的可操作性可降低平台的实施难度。可操作性包括：

- ✧ 灾备平台与用户现有环境的无缝接入能力：AnyVault 平台支持与企业已有网络环境的最大整合能力，既可以支持 LAN、FC-LAN，也支持 LAN-FREE 等备份模式。对于用户现有的 IT 基础也具有很好的支持能力，包括操作系统、应用系统和硬件等良好的兼容性。
- ✧ 灾备平台中用户的自服务能力：在 AnyVault 平台中，具有非常完善的用户管理机制，包括平台管理、企业管理、审计管理和普通用户四级管理模式，平台管理员可以很好的管理平台的运行、运营相关事务，而企业管理员可以直观的管理企业的服务器、PC 的备份与恢复，同时，企业审计管理员可以审计企业的备份行为与数据情况。
- ✧ 灾备管理平台的可访问能力和远程管理能力：企业管理员可以通过 WEB 远程管理企业的所有服务器和 PC 的备份与恢复，一体化管理模式，极大的提升平台的管理能力。
- ✧ 灾备平台的自动化能力和自我修复能力：AnyVault 平台具有很好的自动化能力和自我修复能力，平台的备份、管理简单自动，定时计划任务、基于事件触发备份、实时备份等能更自动的保护客户端的数据。同时，客户端执行多进程化和服务器端的进程容器化很好的保证了系统在发生局部问题时，可以自动修

复，回收资源。

- ✧ 用户界面友好性和界面的完全本地化：AnyVault 基于 ALL-in-ONE-Web 的设计模式，人机交互体验非常友好。

7.3 平台定制研发响应速度

灾备平台用于满足多用户的灾备需求，其必然会存在平台定制的研发，诸如为了满足计算机等级保护制度而定制的分级数据管理措施。

定制研发的内容包括：

1. 满足特定行业法规遵从而作的平台和产品特性开发；
2. 根据客户需求改进性开发和升级，比如对特定应用系统的支持，根据企业客户的需求，添加或者修改客户端功能；
3. 其他定制性开发需求；

爱数 AnyVault 平台具有很好的开放性和适应性，可以根据用户和运营方的需求进行定制化调整，团队的响应速度分为四级：

表 1 AnyVault 平台响应级别

需求与反馈分类	*响应级别*	*响应速度*
新功能需求和反馈	*项目级*	*1 周响应，根据项目计划支持，1 个月左右完成*
改进性需求与反馈	*任务级*	*1 天响应，1 周之内完成*
功能缺陷反馈	*支持级*	*4 小时响应，1-7 天内完成*
特殊需求反馈	*实时级*	*1 小时响应，3 天内完成*

7.4 爱数 AnyVault 平台的可信度

爱数作为国产领先的备份和容灾整体方案供应商，爱数已经获得的安全资质包括：

1. 获得公安部的计算机信息系统安全产品销售许可；
2. 通过国家保密局的涉密信息系统检测；
3. 获得军用信息安全产品认证。

产品的安全性和信息保密性完全既可以可用于企业，也可以应用于政府、证券、医疗卫生、电力等行业的远程数据灾备平台。并且，作为一个国产厂商，研发队伍可迅速响应灾备平台的定制需求，平台的可操作性，特别是用户界面的友好性和完全本地化的界面可充分胜任远程数据灾备平台建设的要求。

第八章 AnyVault 平台功能

8.1 备份恢复功能

- ✧ 全面保护能力：可支持操作系统、应用系统、文件三层备份和恢复。
- ✧ 平台支持能力：可支持 Windows、Linux、AIX、HP-UX、Solaris 等 32/64 位版本的操作系统以及 VMware、Windows Hyper-V 等虚拟环境。
- ✧ 操作系统备份和恢复：
  - ✓ 可支持 32/64 位的 Windows 和 Linux 系统在线增量备份；
  - ✓ 基于 AnyRestore 系统恢复技术，即使硬盘损坏或其它部件损坏，也可将原系统备份集恢复到新硬件环境中。
  - ✓ 支持 IBM、HP、Dell 等各种服务器环境的灾难恢复，包括 RAID0、RAID1、RAID5 等各种 RAID 硬件。
- ✧ 应用系统备份和恢复：
  - ✓ 支持 32/64 位 SQL Server 数据库系统的在线备份，包括完全、增量和事务日志备份等。
  - ✓ 支持 32/64 位 Oracle 数据库、表空间、归档日志的完全、增量备份。支持 Oracle 数据库的时间点回溯恢复，可在已备份时间点的基础上，更精确回溯到某一时间点。
  - ✓ 支持 32/64 位 Lotus Domino 数据库的热备份，包括完全、事务日志备份；支持时间点恢复。
  - ✓ 支持 32/64 位 Exchange Server 邮件服务器的在线备份和恢复。包括对整个数据库或数据库的单个存储组的完全、增量备份。支持对公用文件夹存储、邮箱存储的备份和恢复。
  - ✓ 支持 32/64 位 Sybase 11.0 以上版本的数据库在线备份和恢复。支持系统数据库和用户数据库的完全、增量备份。
  - ✓ 支持 32/64 位 Active Directory 的备份和恢复。
  - ✓ 支持 32/64 位 DB2 数据库系统的在线备份，包括数据库的全备份、表空间备份和增量备份。
  - ✓ 支持 32/64 位 SharePoint（含 WSS 服务）内容数据库的在线备份，包括服务器场以及配置数据库和管理中心内容数据库的完全和增量备份。
  - ✓ 支持 My SQL 数据库的在线备份，包括完全备份和增量备份。
- ✧ 文件备份和恢复：
  - ✓ 支持文件的定时和实时备份。
  - ✓ 文件定时备份可支持增量备份、完全备份、合成备份、循环备份。
  - ✓ 实时备份可支持连续的备份和时间点版本控制，支持块级增量备份，每次仅传输实时变化的数据块。
- ✧ 灵活的计划任务管理，可支持单任务多计划循环周期性备份，包括每隔数小时、每天、每周等。
- ✧ 支持网络备份和恢复的断点续传，网络临时中断，客户端掉电，可在断点处继续备份和恢复。
- ✧ 支持双机环境和集群环境下数据库的断点自动切换续备。
- ✧ 支持 DAS、NAS、SAN 等各种存储结构，支持 LAN-Free 备份方案。
- ✧ 支持 One-PASS 恢复，在恢复时间点数据时，交叉时间点的数据只需要遍历恢复一次。
- ✧ 支持多种恢复方式，包括客户端恢复、下载恢复、搜索恢复等。

8.2 重复数据删除功能

- ✧ 内置重复数据删除功能，支持文件、系统和各种数据库的重复数据压缩，压缩比可高达 300:1 倍。
- ✧ 以任务为单位配置重复数据删除方式，支持网络传输前和网络传输后重复数据删除。

8.3 身份管理和安全性功能

- ✧ 划分为系统管理员、审计管理员、企业管理员、企业用户四级用户权限类别。
- ✧ AnyVault 以企业为基本管理单元，赋予企业管理员权限，可管理一个企业的备份计划和恢复。
- ✧ 支持基于密码、基于 USB-Key、基于密码和 USB-Key 三种用户认证方式。
- ✧ 灾备中心的服务器运行在虚拟的企业上下文环境，可完全隔离备份数据、权限控制、企业元数据等。
- ✧ 备份数据和恢复数据在传输过程经过 Blowfish 和 SSL 双层加密。
- ✧ 支持令牌管理，采用公钥密码技术实现令牌的 CA 认证和安全备份。

8.4 数据管理功能

- ✧ 支持备份数据的在线管理和离线管理。
- ✧ 在线备份数据管理包括恢复、审查、删除、归档等。
- ✧ 采用分级存储管理策略，可定期将某时段的备份数据归档到磁带，离线保存。
- ✧ 可在合成备份时，将符合策略的已过期数据自动归档到磁带，离线保存。
- ✧ 可透明管理缓冲在缓冲服务器上的备份数据，采用全局虚拟文件系统技术，缓冲服务器上的数据在在线备份数据管理为统一视图。

8.5 介质管理功能

- ✧ 采用虚拟介质池组织所有可用的介质服务器、缓冲服务器及其可用介质。
- ✧ 虚拟介质池虚拟为单一介质，供用户透明使用，用户不再需要进行介质管理。
- ✧ 系统管理员可采用集群或群组方式添加新介质服务器到虚拟介质池中，用于空间和吞吐扩展，不需要企业管理员参与。
- ✧ 企业管理员可添加本企业的缓冲服务器到虚拟介质池中，用于缓冲备份数据。
- ✧ 虚拟介质池提供集中介质空间管理，平台管理员可集中管理、查看和分配介质空间。
- ✧ 企业管理员可在分配的介质空间范围内进一步进行介质空间管理，向企业用户分配可用空间。

8.6 灾备中心端架构功能

- ✧ 灾备中心端划分为多个不同角色的服务器，可采用数据库集群技术、LVS 集群、介质服务器群组实现灾备中心的扩展和高可用。
- ✧ 灾备中心备份数据存储可采用 SAN、NAS 或 Lustre 集群，以满足高吞吐和大容量扩展。

8.7 审计功能

- ✧ 可满足《计算机信息系统安全保护等级划分准则》中，第二级系统审计保护级要求：本级的计算机信息系统可信计算基实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。
- ✧ 设有专门的审计管理员，可独立于系统管理员，审计系统行为。

- ✧ 支持用户访问、数据备份、数据恢复、备份数据在线和离线管理、介质服务器扩展和维护等操作的审计。

8.8 报表和告警管理功能

- ✧ 丰富的报表功能，提供备份概况报表、客户端安全状态报表、任务报表、介质空间报表等，完全可视化管理平台的备份状态。

图 6 AnyVault 报表功能

- ✧ 报表可支持多种图形的显示、打印、生成为 PDF 报表。
- ✧ 详尽的日志，划分为系统日志、企业日志、用户日志、客户端日志等。
- ✧ 日志管理可支持 PDF 导出、日志过滤和自动清理等高级特性。
- ✧ 支持 Email 自动告警，可将设定的报表、严重日志事件等自动发送给相关负责人，并且可支持不同接收策略、多接收者。

8.9 缓冲服务器功能

- ✧ 缓冲服务器与企业绑定，一个企业可允许使用一个或多个缓冲服务器。
- ✧ 缓冲服务器用于实现脱机备份、LAN-Free 备份、重复数据删除和缓存加速。
- ✧ 恢复数据时，优先从缓冲服务器上读取数据，可达到灾难恢复时与本地恢复相匹配的速度。
- ✧ 与重复数据删除功能的集成，客户端数据备份到缓冲服务器后才进行重复数据删除，并远程传输到灾备中心。

8.10 其它功能

- ✧ All-in-ONE-Web，AnyVault 平台的所有功能都在一个 Web 中心配置和管理，可方便不同用户随时随地访问和维护。
- ✧ 用户端可部署 LDAP 助手，与 Windows Active Directory 的用户对象实时同步，实现在远程数据容灾时，可与用户现有的身份认证机制完全统一，从而显著提高系统平台的可管理性和安全性。

第九章 AnyVault 平台关键技术

9.1 备份恢复引擎

AnyVault 采用“AnyLink 执行引擎”技术作为备份恢复引擎，该引擎通过一套源代码将备份恢复、重复数据删除、簇照、快照等功能融合，为不同类型的数据，如文件、数据库、邮件等提供统一的备份和恢复能力。在 AnyLink 执行引擎中，将分成三大模块，分别为：Schedule（调度）、Source（源端）、Media（介质端），以实现统一备份和恢复引擎的目标。

图 6　AnyLink 备份原理

AnyLink 引擎自从 2002 年开发以来，已历经大范围的应用检验，其技术能力也在不断发展和前进，目前 AnyLink 引擎的技术支持包括：

- ✧ 广泛的平台支持能力：支持 Windows、Linux、Solaris、IBM AIX、HP-UX 等操作系统，支持 x86、x64、IA64、SPARC、UltraSPARC、PA-RISC、PowerPC 等 CPU 体系结构，支持 VMware Virtual Infrastructures、Windows Hyper-V、Xen 等虚拟化环境。
- ✧ 完善的应用支持能力：支持 SQL Server、Oracle、DB2、Exchange Server、Lotus Domino、Sybase、Active Directory、SAP、SharePoint、My SQL、Postgre 等应用系统。
- ✧ 全面的备份能力：支持周期性备份和持续数据备份 CDP，支持增量备份、完全备份、差异备份、合成备份、循环备份、脱机备份等备份方式。
- ✧ 强大的恢复能力：支持多版本的虚拟时间点恢复、One-PASS 恢复、搜索恢复，以及 CDP 备份的瞬时恢复。
- ✧ 值得信赖的加密机制：数据备份打包和存储时支持 AES、Blowfish 等多种高强度加密，并且在传输过程中 EDTP 协议可支持 SSL 安全套接字 ,在网络链接传输时经过多重加密从而保证备份和恢复的安全可靠。

9.2 重复数据删除技术

远程数据灾备平台采用广域网实现异地的数据容灾，其特性是网络建设投资少，但也导致网络带宽成为容灾平台的瓶颈技术，因此，重复数据删除技术是 AnyVault 平台中最富有创造力的技术。

重复数据删除也称为“单实例存储（Single Instance Repository，简称 SIR）”或者容量优化（Capacity Optimization），是一种数据缩减技术，通常用于基于磁盘的备份系统，旨在减少存储系统中使用的存储容量。它的工作方式是在某个时间周期内查找不同文件中不同位置的重复可变大小数据块。重复的数据块用指示符取代。高度冗余的数据集(例如备份数据)从数据重复删除技术的获益极大;用户可以实现 50 比 1 至 300 比 1 的压缩比。而且，重复数据删除技术可以允许用户的不同站点之间进行高效，经济的备份数据复制。

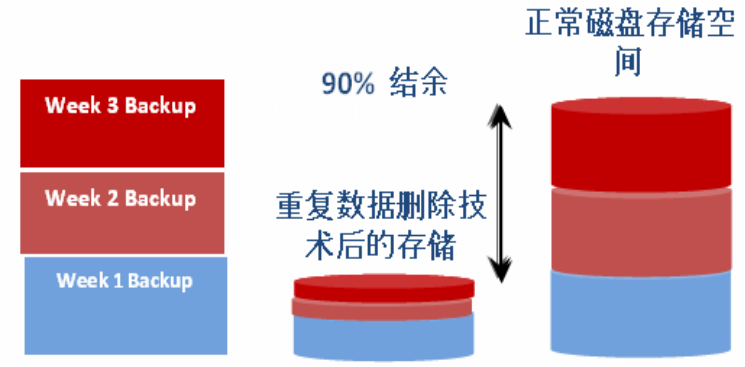


图 7 重复数据删除压缩示意图

AnyVault 平台中采用的重复数据删除技术是基于内容识别的重复数据压缩算法（见专利 200710047904.X 和 200810037869.8），该算法将数据类型识别为一个数据压缩对象，并建立学习机 - 分析机 - 压缩机模型，通过学习机预先学习，将数据压缩对象的存储关联性进行学习，学习过程采用 Rabin 指纹算法、Delta 差异算法、TTTD 算法以及最小上限法等，并将学习结果预存起来，以便分析机和压缩机在备份过程直接使用学习结果高效识别重复数据，从而大大提高压缩比率，并减少压缩所花费时间。

下表为 AnyVault 中重复数据删除压缩比的测试结果，该测试环境中：

- *SQL Server、Oracle 数据库的原始数据量在 10GB 左右；*
- *数据库的每一次的变化量在 500MB 左右；*
- *每次进行完全备份；*

表 3 SQL Server 重复数据压缩比测试结果

测试序号	*数据源大小*	*备份数据大小*	*压缩比*
1	*10GB*	*3.12GB*	*3.2*
2	*10.5GB*	*131MB*	*82.07*
3	*11GB*	*134MB*	*84.05*
4	*11.5GB*	*147MB*	*80.1*
5	*12GB*	*141MB*	*87.1*
6	*12.5GB*	*144MB*	*88.89*
7	*13GB*	*149MB*	*89.34*
8	*14GB*	*152MB*	*94.31*
9	*14.5GB*	*163MB*	*91.09*
10	*15GB*	*166MB*	*92.53*

表 4 Oracle 重复数据压缩比测试结果

测试序号	*数据源大小*	*备份数据大小*	*压缩比*
1	*10GB*	*2.74GB*	*3.65*
2	*10.5GB*	*119MB*	*90.35*
3	*11GB*	*126MB*	*89.4*
4	*11.5GB*	*134MB*	*87.88*

5	*12GB*	*137MB*	*89.7*
6	*12.5GB*	*139MB*	*92.09*
7	*13GB*	*143MB*	*93.09*
8	*13.5GB*	*151MB*	*91.54*
9	*14GB*	*159MB*	*90.16*
10	*14.5GB*	*162MB*	*91.65*

9.3 持续数据保护（CDP）

持续数据保护 CDP（Continuous Data Protection）的关键词是持续。理想的 CDP 技术针对给定的数据集而言，它能够提供恢复点的连续体，能够存取任何时间点上的数据，而不仅仅针对那些由快照流程预先确定的特殊时刻。CDP 允许应用恢复到特定的时间点之前，而不是恢复到预先确定的时间点上。恢复点在时间发生后选定并动态重建。它提供了 粒度无限的恢复点（RPO），有些情况下可以提供接近即时的恢复时间（RTO）。

图 8 CDP 示意图

CDP 技术侧重点不仅仅是在于备份，更重要的一点是瞬间恢复，CDP 的无缝恢复技术能够实现一定业务连续性指标，这是传统的备份技术所不具备的。现在的容灾体系当中，RPO 和 RTO 成为了最重要的两项指标。RPO 是指的是在故障发生之后，希望数据保存的时间点指标，RPO 越小表明数据丢失越小。CDP 技术能够确定 RPO 指标，可以按照用户的要求，恢复到指定的时间点。能够为各个类型的企业，提供不同类型的数据的保护机制和系统保护机制。

AnyVault 平台中提供多种 CDP 或准 CDP 技术提高 RPO 和 RTO 目标：

- ✧ 准 CDP，可支持瞬时恢复：在该技术方案中，采用 VSS 框架可实现数据库的持续数据保护，可支持 SQL Server、Exchange Server、Oracle、Active Directory、SharePoint 等关键应用，并可支持瞬时恢复。

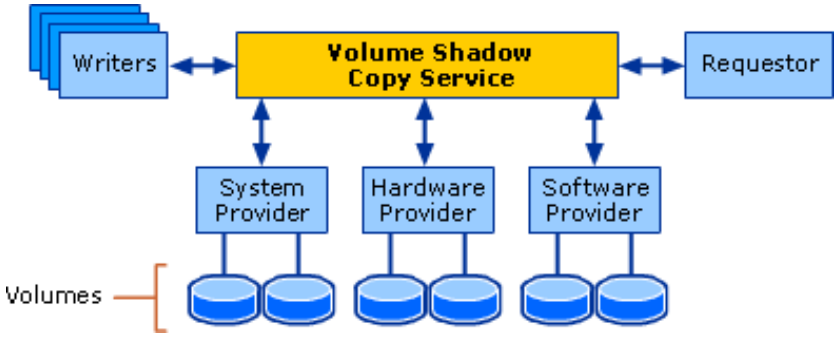


图 9 基于 VSS 框架的 CDP 示意图

但 VSS 框架的应用有一定局限性，仅支持 Windows 2003 及以上的平台。

- ✧ 完全 CDP，仅支持文件系统：完全监控文件系统的变化，实时捕捉每一个时间点并将变化记录下来，可

恢复到任意时间点，然后采用爱数专用技术簇照技术琐定文件变化的簇，以解决备份时因数据变化而导致的备份数据和原始数据的不一致问题。

9.4 网络传输优化技术

在 AnyVault 平台中，备份和恢复数据传输的关键协议为 EDTP 协议，该协议专门用于备份和恢复数据的传输优化，特别是广域网高延迟网络。其关键算法是采用异步多路分帧技术，在广域网高延迟网络环境中，网络带宽使用率可达到 90%以上。

除此之外，EDTP 协议还在协议级支持断点续传特性，当网络发生临时性中断，协议传输栈将保留直到网络恢复连接，协议级断点续传可保证无论是备份还是恢复，包括文件、各种数据库等都能够实现断点续传的特性。

下图为 4Mbps 带宽广域网环境下，AnyVault 平台的备份和恢复带宽利用率，该带宽条件下理论最大传输速度为 512KB/s。在该测试环境中包括大文件和一组小文件测试，其中大文件大小为 1008.7MB，一组小文件为 273 个文件，1.01GB 大小：

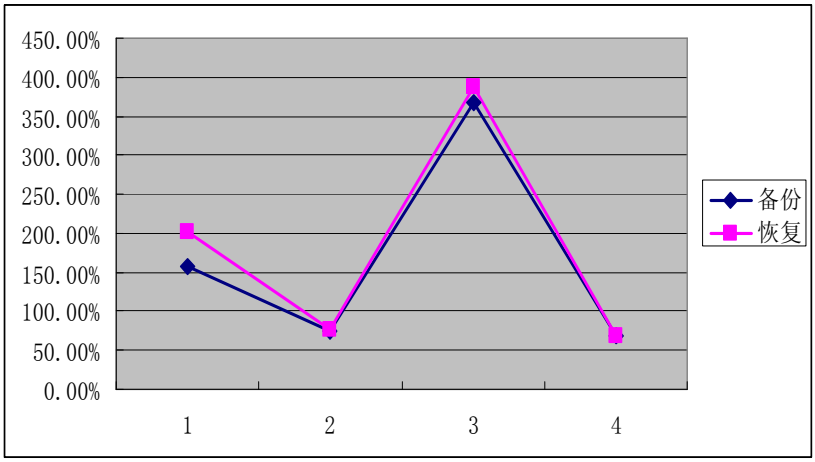


图 10 网络传输测试曲线图

备注：

- *数据 1 为单个大文件在应用标准 LZ77 压缩算法下备份和恢复的带宽利用率。*
- *数据 2 为单个大文件未采用任何压缩算法下备份和恢复的带宽利用率。*
- *数据 3 为一组小文件在应用标准 LZ77 压缩算法下备份和恢复的带宽利用率。*
- *数据 4 为一组小文件未采用任何压缩算法下备份和恢复的带宽利用率。*

9.5 SmartMove 合成备份算法

合成备份用于在介质端将文件完全备份、增量备份等多个时间点合成为一个完整的安全备份，因此不会占用客户端的系统资源，也不会占用客户端与介质服务器间的网络资源。如此可节省备份的数据量，缩短备份窗口，减小客户端压力和网络资源占用。合成备份作为一种优化的备份方式在 AnyVault 平台中应用，每次仅在灾备中心的介质服务器上合成完全备份，不需要客户端重新传输备份数据，也是一种网络传输优化的备份技术。

目前市场上主流备份软件大部分都支持合成备份，但是，他们支持的合成备份在功能和性能上都有局限性。AnyVault 平台中采用改进的 SmartMove 合成备份（专利号 200810207619.4），除了合成范围和合成方式更丰

富，如支持一次性、日、周、月范围内的完全或增量的合成，其性能更是出类拔萃：

- *测试环境：Windows 2003、Intel Pentium Dual CPU 2.00GHz 2G 内存*
- *测试数据：普通文件（TXT、WORD、RAR 等）完全备份大小 18GB、10 次增量备份，平均大小为 300MB。*
- *测试方式：在同等环境和测试数据下，分别执行 6 次合成备份。*

Symantec Backup Exec 12.5D

项目	第一次	第二次	第三次	第四次	第五次	第六次
合成备份时间	912 秒	883 秒	894 秒	920 秒	857 秒	849 秒
最高 CPU 占用率	74%	69%	72%	63%	71%	74%

CommVault Simpana 7.0

项目	第一次	第二次	第三次	第四次	第五次	第六次
合成备份时间	1357 秒	1388 秒	1442 秒	1528 秒	1493 秒	1377 秒
最高 CPU 占用率	61%	63%	59%	59%	61%	65%

爱数 AnyVault 2.0

项目	第一次	第二次	第三次	第四次	第五次	第六次
合成备份时间	87 秒	91 秒	97 秒	94 秒	93 秒	103 秒
最高 CPU 占用率	25%	27%	26%	25%	27%	26%

通过以上测试数据表明，Backup Exec 的平均合成速度为 885 秒，平均最高 CPU 占用率为 70.5%；Simpana 的平均合成速度为 1430 秒，平均最高 CPU 占用率为 61.3%；而爱数 AnyVault 平均合成速度为 94 秒，平均最高 CPU 占用率为 26%，在 CPU 占用率更低的情况下，速度是 Backup Exec 的 9.4 倍，是 Simpana 的 15 倍。

SmartMove 出色的性能取决于专利级的合成备份算法的改进，它根据介质可用空间、已过期数据和无效数据三个权值作为判断合成备份数据完全移动条件，从而使得相对于传统的合成备份算法性能显著提高。

9.6 集群与群组

集群和群组是两种在服务器端规模化的技术，它们都可用于负载均衡（Load Balancing）和高可用（High Availability），以满足大规模用户并发和高性能存储要求。：

在 AnyVault 平台的灾备中心中，包括六大服务器集群和群组：

- 数据库服务器：用于存储平台配置信息，包括用户配置、任务、日志等，可采用数据库集群技术（MySQL Cluster）实现数据库高性能存储、负载均衡以及高可用。
- Web 服务器：AnyVault 平台以 All-in-ONE-Web 特性而简化平台管理，Web 服务器用于提供 Web 访问和平台管理，可采用 LVS 集群实现基于 Apache 的 Web 服务器的规模化。
- 引擎服务器：引擎服务器用于用户管理、任务调度等，是 AnyVault 平台的管理组件，可通过用于用户漂移的群组均衡算法实现引擎服务器的处理能力和高可用。
- 介质服务器：用于实现虚拟介质池，保存备份数据到虚拟介质池，可支持 LVS 集群和群组两种模式，采用 LVS 集群模式时，数据存储池需采用统一存储，而采用群组模式，则既可每台介质服务器介质独立组成一个完整的虚拟介质池，也可采用统一存储。

- ✧ 恢复服务器：用于接受恢复请求进行数据恢复，可采用 LVS 集群实现恢复处理能力和高可用性。
- ✧ 数据存储池：用于储存备份数据，如果介质服务器采用 LVS 集群，数据存储池须采用 SAN 或 Lustre 集群统一存储，如果介质服务器采用群组，则数据存储池可采用 DAS、NAS、SAN 或 Lustre 等存储结构。

9.7 虚拟介质池和缓冲服务器

缓冲服务器是 AnyVault 应用中核心组件之一，它的作用包括：

- ✧ 脱机备份：部署在生产系统同一网络环境中，可实现生产数据的脱机备份，避免远程数据灾备过程对生产系统的带来长时间的性能负荷。
- ✧ LAN-Free 备份：缓冲服务器可部署在 SAN 环境中，轻松实现 LAN-Free 备份方式，然后再通过缓冲服务器与灾备中心的网络链路传输到灾备中心，避免远程数据容灾对生产环境的 LAN 带来网络带宽压力。
- ✧ 缓存加速：采用基于优先级的路径访问算法，缓冲服务器访问路径优先级最高，从而保证在恢复时，总是优先从缓冲服务器上读取数据，从而达到远程数据灾备保有本地恢复的性能指标。

引进缓冲服务器组件后，为了避免缓冲服务器的应用给部署和管理带来更多复杂性，AnyVault 采用虚拟介质池（VMP）将灾备中心的介质服务器和缓冲服务器在逻辑上视为单一介质，并采用全局虚拟文件系统（GVFS）技术，实现介质服务器和缓冲服务器备份数据的单一路径统一访问：

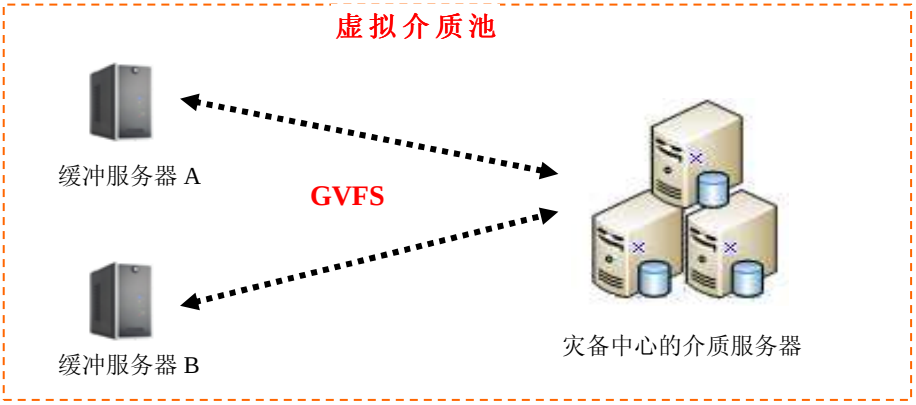


图 11 虚拟介质池示意图

如上图所示，其特性如下：

- ✧ 简化管理，无缝扩展：虚拟介质池将灾备中心的介质服务器以及用户环境的缓冲服务器视为单一逻辑介质—虚拟介质池，用户应用 AnyVault 实施远程数据容灾时，不需要考虑选择什么介质，虚拟介质池可实现免介质管理，根据优先级的路径访问算法选择最佳介质保存数据。
- ✧ 介质漂移：虚拟介质池还支持备份数据在介质中的漂移，一旦某一介质空间使用已满，不中断备份而是漂移到下一可用介质继续备份，从而实现了存储介质的无缝扩展。
- ✧ 缓存同步：虚拟介质池之间可应用缓存同步技术基于备份事件的实时同步，以实现缓冲服务器与介质服务器、介质服务器之间的数据容灾。
- ✧ 基于优先级的访问模式：在虚拟介质池中，采用全局虚拟文件系统，统一虚拟文件路径，以实现备份数据的随处访问。采用基于优先级的路径访问算法，该算法在使用虚拟文件路径访问时，优先从权值高的服务器中读取数据，以便当备份数据保存在缓冲服务器中时，读取数据优先从缓冲服务器中读取，在恢复时可达到本地恢复的性能要求。

9.8 缓存同步技术

在 AnyVault 平台中，缓冲服务器的作用既用于实现本地备份，又用于加速和压缩远程传输的数据，其中缓冲服务器无缝集成到 AnyVault 平台中应用的关键技术为缓存同步技术。该技术应用爱数的专利技术（专利号200810203226.6），实现将缓冲服务器上的备份数据高效可靠地传输到 AnyVault 平台中的虚拟介质池中。

AnyVault 缓存同步技术引进如下关键算法以保证可靠高效的同步备份数据：

- ✧ 备份事件（Backup Event Synchronization）算法：不同于 IO 同步算法，缓冲服务器仅侦听变化的备份事件，根据备份事件变化的操作对象进行同步，特别是合成备份事件，可将合成备份事件的操作对象同步到远程灾备中心，从而避免将合成的备份数据重新传输到远程灾备中心。
- ✧ 瞬时内存缓冲（Instant Memory Cache）算法：缓冲服务器在启动时初始化一块内存映像区，用于保存缓冲服务器上变化的备份事件，该算法可防止网络意外中断、缓冲服务器掉电停止时，已传输数据的进度信息丢失，从而实现同步数据的断点续传。
- ✧ 灰色对象检测（Gray Object Detection）算法：将缓冲服务器上侦听到变化的备份事件中的操作对象视为可同步和不可同步两种状态，当操作对象不可同步时，视为灰色对象。在缓存同步技术中可控制灰色对象的存活时间，一旦在指定的存活时间中灰色对象仍然不可同步，则丢弃此灰色对象，从而避免单一对象同步出现故障后，整个缓冲服务器上的数据被阻塞。
- ✧ 层叠增量（Cascading Increment）算法：缓存同步在备份容灾平台应用时，由于同步到远程灾备中心的带宽处理能力远远小于内部网络的带宽处理能力，从而正常备份状态下，大量的备份事件保存在内存映像区。层叠增量算法用于将操作对象相同的事件进行合并，从而减少冗余无效事件的同步，可显著减少网络传输的数据量。

9.9 安全认证技术

AnyVault 平台的灾备中心通过 Internet 广域网向用户提供远程数据灾备服务，因为平台暴露在 Internet 广域网上，因此对安全性要求很高。AnyVault 平台采用了如下一些安全认证技术：

- ✧ Double-Security 级数据加密：数据备份打包和存储时支持 AES、Blowfish 等多种高强度加密，并且在传输过程中 EDTP 协议可支持 SSL 安全套接字，在网络链接传输时经过多重加密从而保证备份和恢复的安全可靠
- ✧ 强身份认证：强认证正是安全界为解决密码认证存在的种种不足而推出的下一代安全新标准。为用户访问内部和网络数据提供安全可靠的方法。AnyVault 可支持 USB-Key、数字证书等强身份认证方式。

- ✧ 基于公钥密码技术的 CA 认证和安全备份（专利号200910046064.4）：生成身份令牌时，采用公钥密码技术将私钥保存在 AnyVault 平台的身份令牌管理单元，而将私钥保存在身份令牌中。在登录和备份过程中，根据身份令牌中的用户信息和公钥生成 CA 数字签名，进行身份认证以及备份密钥加密传输。
- ✧ 企业上下文（Enterprise Context）：在 AnyVault 灾备平台中，引擎服务器、介质服务器等都运行在虚拟的企业上下文环境，每一个企业上下文都包含权限信息、使用元数据，用户令牌信息等，不同企业的上下文环境采用逻辑隔离，以保证每一个企业的安全性都完全独立，不会受到关联性影响。

结束语

随着中国电子政务、电子商务和企业信息化的发展，大型的政府数据中心、行业数据中心和企业数据中心也已经陆续建成，并且对数据中心基础设施的需求仍然持续高涨。在经历了一系列的信息安全事故和各种灾难事件之后，中国各级政府和重要行业的主管部门已经充分认识到：基于数据中心的远程数据灾备平台，是构建信息安全保障体系的重要组成部分，因此已经制订了一系列有关信息安全和灾难备份的发展规划与应用标准。

专业化得数据灾备平台需要有专业化的建设方案，本书是爱数集多年的备份与容灾的建设经验的精粹所在，从平台建设、功能到技术，爱数都有着成熟的解决方案和成功案例，包括与国内最大的中立 IDC 运营商合作建设和开发的云备份服务平台。

爱数 AnyVault 容灾平台是创新性的新一代企业级远程数据灾备平台，如上所述，无论是 AnyVault 概述与分析，平台功能、部署与实施，均说明采用平台化的容灾系统才能满足远程数据灾备平台的建设目标。

1. AnyVault 平台具有高可用性：平台可以彻底解决远程灾备的网络瓶颈问题，采用基于全局的重复数据删除技术，既减少了存储数据量，又摆脱了大量重复数据传输的问题。采用本地脱机备份+远程异地容灾的服务模式，既可以满足高速容灾，也真正解决了快速恢复问题。同时，AnyVault 是真正的满足大数据量、大并发客户端容灾备份的百万级并发平台。
2. AnyVault 平台具有可运营性：平台适应与各种服务器的容灾备份、具有基于企业为管理单元的服务支撑能力和高可扩展能力，是业界唯一可用于大规模运营的容灾平台。
3. AnyVault 平台风险具有可控性：包括备份审计制度、报告机制和预先告警机制等等，既能解决平台运营的风险，也能满足企业容灾备份的业务连续性风险要求。
4. AnyVault 平台符合国家法规：容灾平台的 RTO 和 RPO 均满足国家信息系统灾难恢复的 4-5 级要求，符合规范对于数据容灾的标准。平台具有非常高的安全性，获得国家多项涉密资质认证，产品稳定可靠。

EISOO 爱数
安 全 备 份 存 储

上海爱数软件有限公司
上海市闵行区联航路 1188 号浦江智谷 10 号楼 2 层
Tel: 021-54222601
Fax: 021-5432 6440 - 8118
www.eisoo.com

了解更多

要了解更多最新产品、推荐解决方案和购买信息请联系爱数销售业务代表，更多信息请登陆爱数官方网站 www.eisoo.com。