国家教育信息管理系统

解决方案

成都天心悦高科技发展有限公司

2013 年 9 月

声明

- **未经成都天心悦高科技发展有限公司书面许可，本解决方案任何部分的内容不得被复制或者抄袭用于任何商业目的。**
- **本解决方案的内容在未经通知的情况下可能发生变化。**
- **如有任何意见或建议，请通过下述方式与本公司取得联系：**

  公司网站 http://www.tianxinyue.com

- **公司电话 028-83318559 邮箱 tianxinyue@126.com**

目录

1 引言

教育管理信息系统建设是教育信息化重点任务之一，其核心内容是建设国家教育管理公共服务平台，建立覆盖全国各级教育行政部门和各级各类学校的管理信息系统及基础数据库，为加强教育监管、支持教育宏观决策、全面提升教育公共服务能力提供技术和数据支撑，对实现教育管理现代化具有重大意义。为此，教育部、财政部等联合下发了促进教育管理信息系统建设的通知。但是，旧有方案在多个方面无法满足当前形势发展的需要，因此需要提出更好的、更全面的、能够满足国家安全需要的解决方案。

“斯诺登”事件彻底暴露出我国信息化系统大量采用外国硬件和软件产品的弱点。正是由于在核心的信息化系统中大量采用外国产品，才使得我国的信息化系统对某国情报部门完全透明。国家领导部门已经认识到这个问题的严重性，并要求全面采用国产化产品来构建自己的信息化系统。在这种形式下，以外国公司的硬件设备、操作系统、数据库、云计算平台、应用服务器等为核心的解决方案已经无法满足国家安全的需求，必须推出以自主产品、国产化产品为核心的解决方案，并采用创新性、基础性的安全技术，才能满足国家信息化系统安全的需要。

像国家教育管理信息系统这样重要的核心系统，不仅仅要保证信息安全，如何确保系统不因各种故障或者自然灾害而损毁，也是非常重要的问题。传统的以集群和数据备份为主的容灾手段显然无法满足需求。它们只能解决单个设备产生的故障，无法应对像大面积停电、火灾、网络故障等更大一些的灾难，更不要说战争时期的恶意打击。因此，如何建设出自然具有抗毁容灾能力，无需单独为容灾投资的系统，就是本解决方案将要回答的问题。

除了安全、抗毁容灾外，如何更好的满足覆盖全国的教育管理信息系统的大业务量、业务多样化等需求，如何解决好网络汇聚流量过大问题，如何更充分的利用各种资源，如何提升应用体验好感度（如网络延迟大，响应慢就是不好的体验）等，也是本解决方案将要考虑的问题。

2 参考文献

（1）国家教育管理公共服务平台省级数据中心建设指南，教育部教育管理信息中心编制，2013 年 4 月；

（2）国家教育管理信息系统建设总体方案(印发稿)，中华人民共和国教育

部，2013 年 7 月。

3 原有解决方案存在的问题

3.1 原有解决方案简述

根据《国家教育管理信息系统建设总体方案》和《国家教育管理公共服务平台省级数据中心建设指南》，原有解决方案拟建设各自独立的教育部数据中心和各省省级数据中心。以教育部数字中心为最高中心，各省数据中心通过数据交换中间件向上汇聚各种数据。同时，各省数据中心独立地为本省的教育机构提供所有服务，所有省级数据中心完全独立建设，互不相关。

在各个数据中心，采用软件即服务（SaaS）为主、基础设施即服务（IaaS）为辅的模式，以省级数据中心为基础，建设区域教育管理云服务平台。建设指南则进一步明确，服务器系统采用虚拟机技术+负载均衡集群的模式，实现集群式的多虚拟机并行服务，以解决资源共享、业务扩展和提高系统可靠性等问题。操作系统根据国家信息系统部署要求选用 Linux 或 Windows 平台。数据库系统则要求采用 Oracle 或者 SQL Server，利用数据库系统的集群技术提高可用性和服务能力。虚拟化技术没有明确方案，可能的选择包括 VMWare、IBM 的云平台和 Oracle 的云平台，或者国内的云平台产品。

在存储备份方面，则配合服务器虚拟化采用光纤网络存储系统，通过网络存储系统的设备共享和管理功能提供共享的存储系统。数据库系统建议采用双机备份加异地日志复制的容灾方式。WEB 服务器和应用服务器的虚拟机数据只建议复制原始镜像到异地。非结构化文件则基于 IP 网络或磁盘阵列系统的能力，复制全部或部分数据到异地；其他数据则不考虑备份。但这些异地系统都需要在未来再投资建设。

在应用容灾方面，建议在异地建立各类应用系统和数据的完整、实时备份，作为更加完整的容灾系统建设。因需要单独投资建设，建议逐步完成。

在安全方面，由于无法在操作系统、数据库和基础平台等方面进行安全增强，因此主要依靠物理安全和网络安全，加上电子认证和数字证书系统。操作系统和数据库安全仅能依靠微软、IBM 和 Oracle 等国外公司提供补丁和安全服务。

总结起来，原有解决方案以集群和虚拟化技术为核心，大量采用国外系统和软件，如 Windows 操作系统， Oracle 或者 SQL Server 数据库等产品，并将安全建设集中在物理设备、网络和制度方面。操作系统、数据库和云平台的安全则由国外产品供应商负责。

3.2 原有解决方案存在的问题

对原有解决方案进行仔细分析，发现该方案存在抗毁容灾能力不足问题，出口带宽不足而远程访问慢问题，系统扩展能力不足问题以及基础设备和软件大量采用国外产品，安全性差等问题。

3.2.1 抗毁容灾能力不足问题

原有解决方案缺乏全面完善的抗毁容灾解决方案。对数据库系统，仅仅采用本地双机备份方式。建设指南建议的异地 IP 数据库日志复制需要单独建立机房、投入设备和软件等措施在规划中完全没有。同样，各种重要数据仅能在本地通过磁带系统离线备份，所谓的异地复制完全没有规划，因为这需要为每个数据中心单独建设独立的机房和完全相同的系统，需要大量的投入。

很显然，仅仅依靠本地的双机备份和离线备份，在数据中心因为停电、网络故障、自然灾害等无法运转时，整个省的业务就会停止，数据也可能在故障时丢失，造成重大灾难。

如果要提升原有解决方案的抗毁容灾能力，就必须为每个数据中心建设相等规模的灾备数据中心，这就要求增加几乎一倍的投入。显然，这是很难被接受的解决方案。

3.2.2 出口带宽不足，远程访问慢问题

考虑应用全面铺开后，在开学等重要时间节点，每个学校至少需要四五个终端同时录入信息，每个终端的带宽开销至少是 0.2Mbps，因此一个学校的业务流量不应当是 0.1Mbps，而应以 1Mbps 计算。

原有解决方案将全省甚至全国的应用服务，如学籍管理等集中到一个数据中心。这样，对一个有 1 万所学校的省份来说，需要的流量是 10Gbps，而不是 1Gbps。显然，很难在一个信息中心获得这样大的出口带宽，也没有一个运营商网络能够支撑这样的汇聚流量。

旧方案在每个省建立全省集中的信息中心，在教育部建立全国集中的信息中心。这种模式使得大量的用户必须通过互联网络或者教育网远程访问，对像云桌面这样的需要较大网络带宽的应用来说，这种模式根本无法为每个用户提供满足业务要求的带宽，结果必然是又慢又卡。

3.2.3 系统的扩展能力不足

系统扩展包括存储能力扩展、服务能力扩展、出口带宽扩展等。任何一个方面的扩展能力受限，则系统就无法再继续扩展。因此，解决方案必须全面的解决每个方面的扩展问题。

原有解决方案的存储扩展依靠单套系统的扩展能力，其上限就是几百 TB。而且容量达到几百 TB 的单套存储系统价格非常昂贵。参照建设指南，对一个学生数量超过 500 万的省信息中心来说，单是学生学籍信息就是 100TB，而且还会逐年累积。其他各种业务系统也会产生大量的数据。因此，随着时间推移，各种业务扩展，以及新增业务，一个省数据中心的存储需求将远超几百 TB。显然，原有解决方案无法提供这样的存储扩展能力。到时必然新建独立的网络存储系统，这样又形成相互隔离的存储系统了。

原有解决方案对业务量庞大的应用采用负载均衡技术加虚拟机的方式。这种方式只能扩展到本地运行的十多台虚拟机，无法扩展到更大的规模，也无法在多地协同服务，其服务能力仍然有限。实际应用中，操作员将不会间隔 30 秒才提交一次请求，而是平均 10 秒就产生一个请求。考虑高峰时间不是只有 20%的终端在工作，而是 80%甚至全部的终端都在工作，而且每所学校也不是只有一个终端，则每所学校的所需的 TPC-C 值将是原有估计数据的十倍以上。很显然，原有的解决方案低估了系统的负载需求，而且业务扩展能力也不足以应对业务的不断扩展。

原有方案明显存在出口带宽不足问题。因此，原有方案无法满足全省教育管理业务扩展的需求。总结起来，原有解决方案在各个方面的扩展能力都有限，因此并不能满足教育管理信息系统的扩展需求。

3.2.4 大量采用国外产品，安全无从谈起

原有解决方案大量采用国外硬件和软件产品。尤其是在核心设备、系统软件和基础平台方面采用国外产品，从而将系统安全的核心都交给了国外公司掌握，安全设计也就只能在外围做文章了。

原有解决方案在操作系统上采用 Windows，在数据库上采用 Oracle 和 SQL Server，在虚拟化上采用 VMWare 等国外产品，在应用服务上采用 WebLogic，在 WEB 服务上采用微软或者 IBM 的产品。这些都是信息化系统中最基础、最重要、最核心的部分。如果这些产品中存在安全漏洞或者后门，即使在物理安全、网络安全和安全制度上下再大的功夫，都无济于事。国外情报部门仍然轻松地就

可获得需要的信息。哪里谈得上安全。

4 需求和建设目标

参照《国家教育管理信息系统建设总体方案》的要求，本解决方案需要满足以下需求。

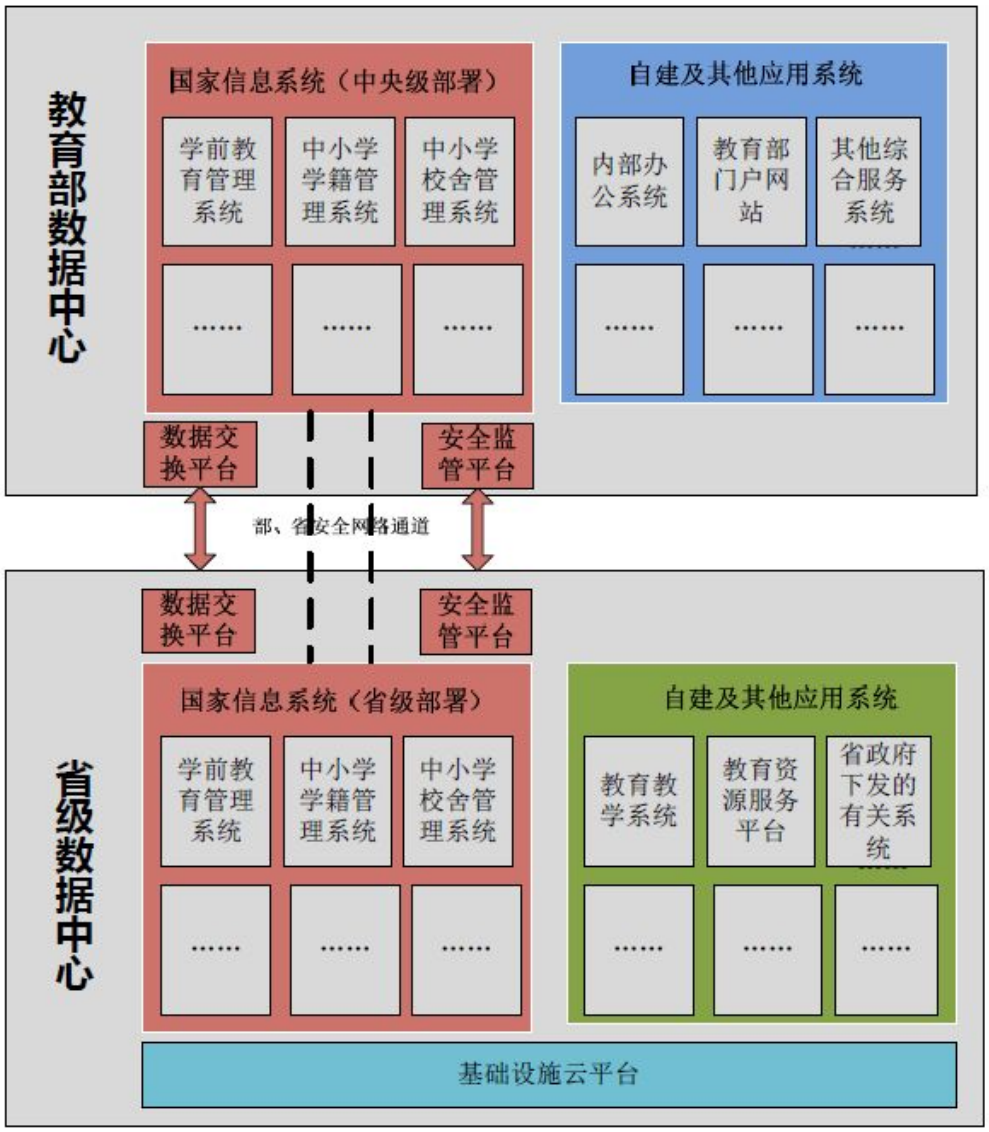

图4-1 国家教育信息系统的应用层次结构

4.1 满足国家教育管理信息系统部署和服务的需要

国家教育管理信息系统是大量应用系统有机整合的服务体系，其应用结构如图 4-1 所示。

它包括多个覆盖全国的应用系统，如学前教育管理系统、中小学学籍管理系统、中小学校舍管理系统等。这些系统采用部、省、市、县、学校五级应用结构。这就要求系统具有良好的服务扩展能力、强大的互联互通能力、高扩展的海量存储能力等等。同时，系统也包括教育部、各省市、甚至各个区县自建的各种应用系统。这些业务系统有大有小，需要的资源量各不相同，因此要求系统具有良好的业务承载能力，优良的业务隔离性和完善的资源动态分配能力，从而既能满足各种业务运行的需求，又能充分利用已有的资源。

4.2 满足建设集中统一的教育基础数据库的需求

教育部文件指出：“建立集中统一的教育基础数据库，纵向贯穿学前教育、中小学教育、中等职业教育、高等教育和成人教育等各个教育层次,形成上下一致的教育机构、学生、教师（职工）、学校资产及办学条件基础数据库；横向打通学生、教师（职工）、学校资产及办学条件数据，形成全面整合、集中一致的教育管理和决策基础数据库，为各类业务信息系统提供数据服务”。

因此，国家教育管理信息平台应当为建设集中统一的教育基础数据库提供支撑。这种支撑不仅仅是提供一个数据库产品，满足各级教育部门数据库服务的需要，也不仅仅是研发一套数据交换软件来交换数据，还需要为建设集中统一的教育基础数据库提供良好的数据共享支持，完善的数据访问管理机制和方便的数据访问手段。

4.3 建立完善的信息化基础设施

建设国家教育管理信息平台的目标不仅仅是运行教育部规定的那些应用，还需要满足教育部、省、市、区县等各级教育部门自有业务运行的需求，为各级教育机构提供公共的业务运行平台、数据存储平台、抗毁容灾平台和安全服务平台等，从而提升资源利用率，减少重复投入，降低使用成本等。

4.3.1 共享的业务运行平台和数据存储平台

本解决方案为各级教育机构、学校提供共享的业务运行平台和数据存储平台。它整合分布在全国各地的各级教育机构建设的大大小小的信息中心，形成一个全国统一的基础平台，为各级教育机构的自有应用提供共享的业务运行平台和数据存储平台。

这个共享的运行平台具有优良智能性和可管理性。通过管理工具，可以限制

各个业务运行的位置，使其运行在管理员希望运行的地方，并只使用分配给它的资源。同时，系统又能智能的选择各个业务运行的地方和服务器，使其获得理想的服务效果，充分的利用各地的计算资源。

本解决方案为各级教育机构提供共享的数据存储平台。各级教育结构的各个业务系统按需从共享的存储系统获得存储资源。这样可以减少存储资源闲置，减少各个单位重复建设，降低系统使用成本。

和旧解决方案不同，本解决方案将整合部署在各地信息中心的所有存储系统，按需分配给系统的各个应用，而不是只在各个数据中心内部对单个存储系统进行共享，从而进一步提升存储资源的利用效率。

本解决方案为各种应用提供共享的文件服务和数据库服务，无需再为各个应用部署独立的数据库服务器和文件服务器，从而减少这方面的投入。

4.3.2 共享的抗毁容灾平台

单独为各个信息中心建设抗毁容灾设施不仅投入大，而且获得的抗毁容灾效果有限。对基层教育机构来说，单独建立抗毁容灾系统更是无法承受的投入。因此，为各级教育机构建设统一的，共享的抗毁容灾平台，提升业务运行的可靠性，是本解决方案不同于其他解决方案的地方。

本解决方案将建设在各级教育机构中的信息中心整合起来，使数据可以在这些信息中心间异地复制，业务可以在这些信息中心间异地运行或者分布式运行，并智能的迁移服务，从而解决所有应用系统的数据和业务抗毁容灾需求，无需额外的容灾系统建设，从而有效地降低成本，且满足各级教育机构的抗毁容灾需求。

由于本解决方案将建设为各级教育机构共享的业务运行和数据存储平台，因此各级教育机构均可将自己的应用部署到这个平台中，从而自然的获得抗毁容灾支撑。即使是基层的一个小学，也无需再为自己的应用停机而担忧。

4.3.3 共享的安全服务平台

本解决方案将为各级教育机构建立共享的安全服务平台。这个平台提供电子认证和数字证书服务、敏感数据加密存储和访问服务、密钥管理服务和数据安全传输服务等，从而满足各级教育机构应用安全的需求。

4.4 建立高效的运行维护系统

运行维护制度、组织结构和队伍的建设只是为系统的稳定运行提供了某些必

要条件。要使系统高效稳定地运行，还需要信息化管理技术的支撑。

本解决方案将为系统建立一个虚拟集中的多级运维管理平台。该平台将管理覆盖到系统的每一个角落，全面监控系统的运行状态，提供实时的图形化的运行状态显示，及时报警，及时获得系统运行日志，并为远程控制提供支持。这将使得管理员能够在控制室全面掌握系统的运行状态，并及时对各种异常做出反应，从而确保系统高效稳定地运行。

本解决方案的运行维护系统包括机房环境监控系统、网络管理系统、服务监控和管理系统、终端设备管理系统、安全监控和管理系统等，从而全面监控系统的各个方面。

这个运维管理系统采用多级管理框架，各级信息中的管理人员均可对本信息中心和下级信息中心的系统进行监控和管理，从而可以减少县市信息中心的运行维护人员，从而减少人员开支。

5 设计原则和基础平台

5.1 设计原则

本解决方案将根据以下设计原则来完成系统的设计。

5.1.1 以国产化产品为核心

没有核心系统的国产化，就没有整个系统安全。因此，本解决方案将以国产化操作系统、数据库、应用平台为软件核心。同时，配合国产化的服务器平台，如龙芯服务器；国产化的网络产品，如华为、中兴、迈普等的网络产品；国产化的安全设备，如天融信的防火墙、启明星辰的入侵检测等。从而构建起以国产化产品为核心的系统平台，确保整个系统的安全性。

5.1.2 将安全做到底层去

没有操作系统和数据库的安全，就没有应用系统的安全。因此，必须将安全做到底层去。本解决方案拟采用具有自主知识产权的、具有创新性安全特性的操作系统和数据库为基础，构建安全的系统平台。摒弃国外的操作系统和数据库产品、如 Windows 操作系统、Oracle 和 SQL Server 数据库等。

5.1.3 全面考虑抗毁容灾

全面考虑抗毁容灾不是要分别为每台设备、每个系统建立容灾机制，而是要全面的，统一的、整体性的考虑整个系统的数据、业务和系统的抗毁容灾，使抗毁容灾成为系统自然的一部分。

本解决方案将抗毁容灾融合到整个系统中去，而不是单独为某台设备、或者某个数据中心建立一些孤立的备份系统，从而全面的满足所有数据、业务和系统的抗毁容灾需求，降低系统的抗毁容灾投入。

5.1.4 建设分散部署、虚拟集中的系统

根据分析，集中部署的形式无法满足业务系统的高带宽需求，也无法获得足够的业务扩展能力来满足应用不断扩展的需求。因此，系统的部署模式必然是多信息中心的。但是，这些分散的信息中心必须在统一的软件平台下进行整合，使其能够集中管理和控制，并以一个整体来满足各种应用的需求。这就是分散部署、虚拟集中的含义。反之，只是分散而无法集中管理和控制的系统，或者集中部署的系统都不是理想的平台解决方案。

5.1.5 全面考虑系统扩展性

根据教育部的规划，这个基础设施需要满足各级教育机构不断增加的应用系统的部署需求，而不是只为当前明确的几个应用提供支持。因此，系统必须具有全面的扩展性，在网络、服务系统、存储设备、数据库、部署地点等方面都要具有扩展性。。

5.1.6 以信息化技术支撑系统运维管理

信息系统的管理不能只依靠维护队伍的人力来完成，而是需要信息化手段来支撑，从而简化管理的复杂度，提升管理效率，减轻管理工作量，最终达到减少管理投入的目标。

为此，需要同步建设系统的管理维护平台，而且这个平台必须能够管理整个系统，而不是各个数据中心管理各自的部分。

5.2 基础平台简介

本解决方案以数字有机体系统为基础。将若干计算机通过宽带网络互联，根据需要采用现有的和最新的理论和技术，使互联而成的系统具有生物抗体之特性，则该系统即为数字有机体系统。通俗一点，数字有机体系统由许多分布于不同地方的数字有机体站组成。每个数字有机体站由高速交换网络、一定数量的服务器，以及它们内置或者外接的磁盘阵列等存储设备构成。在数字有机体系统软件的整合下，每个数字有机体站本身可以独立运行，也可以作为整个系统的一部分参与协作。每个数字有机体站无论大小，在逻辑上都是平等的。因此整个系统没有中心节点或者中心系统，具有良好的自组织性。

数字有机体系统基于开放源代码的 Linux 操作系统研发，从 2000 年开始，于 2004 年推出了第一个版本，并应用于国家 863 项目——填补西部数字鸿沟中的电子政务系统。从 2006 年起，数字有机体系统在成都市人民检察院推广应用。2010 年，成都市人民检察院数字有机体综合信息系统应用获得了成功，并通过四川科技技术委员会的科学技术成果鉴定。专家一致认为“系统具有重大创新性，达到了国际先进，国内领先水平”。

5.2.1 数字有机体系统功能概述

数字有机体系统的逻辑结构如图 5-1 所示。从概念上讲，数字有机体系统是一系列软件构成的系统。其中，系统平台层软件是数字有机体系统核心的部分，它实现了许多现有系统不具备的功能。

图5-1 数字有机体系统的逻辑结构

在系统平台层上，构建了用于支撑各种应用系统的应用支撑层。可以提供流媒体服务、多媒体通信、安全服务和 WEB 服务等支撑。这些应用支撑系统的功能在后面具体应用的时候再详细描述。

数字有机体系统构建了完善的管理维护系统。它覆盖系统的各个层面，包括机房环境、安全监控、设备监管、业务监管、网络管理和终端监控等模块，具有统一报警，图形化展示等功能。

系统平台层是数字有机体系统核心，也最具创新性的部分。在各个模块的配合下，数字有机体系统不仅整合了现有的各种先进软件系统，还具有了许多特有的功能和特性。下面分别描述这些模块的功能和特性。

（1）数字有机体工作平台

数字有机体工作平台是整个数字有机体系统的基础。它主要实现几个方面的功能。

1）系统结构组织：管理系统中分散部署在各地的所有服务器，将其组织起来，形成一套有机的系统。

2）资源管理：管理系统中各种资源，如服务器的计算能力、各台服务器的存储设备、各台服务器的网络带宽等并负责资源的分配和回收。

3）负载均衡：提供全局负载均衡和本地负载均衡。全局负载均衡指在各个信息中心（服务器部署点）间均衡系统负载，并向网络用户提供就近服务调度。本地负载均衡指在一个信息中心内均衡服务器间的负载，使每台服务器都能得到充分的利用。

4）虚拟服务器：这是针对像 WEB 服务这类的应用提供的一种支持，其目的是使网络用户可使用一个服务 IP 地址访问整个系统。它也具有全局负载均衡和本地负载均衡功能。

（2）大规模存储管理系统

大规模存储管理系统包括两个子系统，即存储池管理子系统和数字有机体文件子系统。

存储池管理子系统负责系统中存储设备的管理，包括登记、分配和回收。存储分配还现实了配额机制。该机制将统计每个用户使用的存储空间，并登记每个用户可用的存储配额；在分配存储空间前，检查用户的配额是否充足；即限制每个用户的空间使用量，以防用户滥用存储设备。

和存储池管理子系统对应的是数字有机体文件系统。他的文件就存储在这个存储池中。其主要功能是：

1）多文件系统：每个用户都可在这个文件系统中建立各自独立的子文件系

统。这些子文件系统间相互不可见，即是完全隔离的。

2）分布式存储：每个子文件系统中的文件、目录都分散存储在虚拟存储池中，不受任何单一存储设备的容量限制。

3）文件复制：系统提供数据复制功能。每个完整的复制称为一个副本。对一个文件的多个副本的更新方式除了传统的同步更新和异步更新外，还提供混合更新模式。在该模式下，文件写操作将尝试同步更新所有副本，但只等待设定的最小副本数完成即结束更新，未能同步更新的副本将异步更新。数据更新采用传递写操作日志模式。

4）副本智能管理：对每个文件的副本，系统将智能化管理。这种智能包括：智能地选择副本的存储位置，智能地增减副本数以满足访问需求和可用性需求，智能地迁移副本以满足访问需求等。

5）并发访问：系统提供分布式锁机制，便于用户并发地访问同一个文件或者目录。访问不同的文件和目录无需互斥，因此可以并发进行。

6）独立的文件访问权限系统：建立了独立于任何单一服务器的文件访问权限系统，实现了 Unix 传统的自主访问控制，也支持 SELinux 的强制访问控制。

（3）抗毁容灾系统

数字有机体抗毁容灾子系统和工作平台、文件系统、数据库管理系统等配合，实现了数据、业务和系统三级抗毁容灾。在发生故障时，系统能够确保数据不丢失且可以连续访问，业务能从断点处继续服务，系统能够重构。具体功能介绍参见 6.5.3 节“实现全面抗毁容灾”。

（4）数据库管理系统

数字有机体工作库是一个支持大规模分散部署的数据库系统。其主要功能如下：

1）多数据库管理和透明访问：在这个管理系统中，用户可以创建大量的数据库。这些数据库分散存储在各个服务器管理的存储设备中。但对数据库使用者来说，在权限许可的情况下，他可以从任何一台服务器访问任何一个数据库，无需考虑这个数据库具体存储在那里。

2）分布式事务：系统支持分布式事务，从而满足应用的事务处理需求。

3）异步复制：每个数据库都可进行多副本复制，对多个副本的更新可以采用分布式事务机制，也可采用传输更新日志的异步更新模式。更新日志采用二进制日志和操作语句日志混合模式，系统自动选择每个事务合适的日志模式，通信开销小。

4）智能复制管理。系统能够智能地管理各个数据库的副本。这种智能化体现在选择副本存储位置，增减副本数量和迁移副本位置等。

（5）虚拟机管理系统

数字有机体系统的虚拟机管理系统的框架如图 5-2 所示。

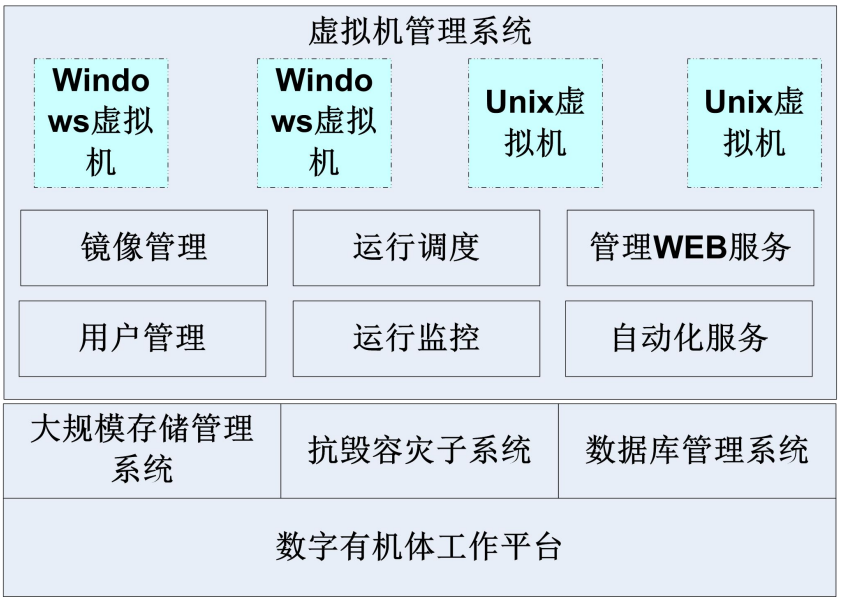

图5-2 虚拟机管理系统的框架

虚拟机管理子系统的底层就是前述的各个子系统。因此系统节点、资源等的管理已经由底层完成，虚拟机镜像文件等的容灾也交由抗毁容灾子系统完成。虚拟机管理子系统的主要功能如下：

1）镜像管理：登记每个业务系统的各个镜像文件，以便在需要时能够找到需要的镜像文件。

2）用户管理：虚拟机管理系统的用户就是数字有机体系统的用户。本模块只管理各个用户的权限，并对用户的虚拟机操作请求进行授权。

3）运行监控：监视每个正在运行的虚拟机的状态，收集运行数据，并对虚拟机运行故障进行处理。

4）运行调度：调度每个业务虚拟机的运行，包括确定运行位置、增减虚拟机数量等。

5）自动化服务：提供像自动在虚拟机中安装操作系统等服务。

6）管理 WEB 服务：提供虚拟机云管理平台的 WEB 管理界面。

（6）安全子系统

安全子系统既有融入前述各个子系统的部分，也有像增强密钥管理服务、统一身份鉴别和授权系统这样的单独模块。从逻辑上讲，安全子系统实现了操作系

统层、数据库层和平台层的各种安全功能。具体请参见 6.3 节“安全框架”部分的描述。

5.2.2 数字有机体系统的特性

数字有机体系统具有三大突破。它第一次提出了分布式并行输入/输出接口的概念，突破了传统系统在 IO 上的瓶颈，从而保证无论有多少客户，无论客户在何处，都能够即时得到服务；其次，它第一次实现了无缝的任务迁移，从而可以在节点出现故障时，仍然保证任务从断点继续执行；第三，在整个数字有机体系统内，在各数字有机体站之间，无大小之分，无高低之分，无中心控制站或节点，在系统范围内提供服务。数字有机体系统具有以下特性：

- 自适应能力

系统具有良好的自适应能力。开始，系统可以仅由三台普通服务器形成一个数字有机体站。当应用需要扩展系统时，可以在线增加服务器，提高单个数字有机体站的服务能力，也可以增建新的数字有机体站，新的数字有机体站在网络连通后，自动融合到已有的数字有机体系统中，成为它的一部分。当系统中的部分节点发生故障时，系统自动重组，形成新的数字有机体系统，保证服务的延续性。

- 自学习能力

系统具有良好的自学习能力。系统能够通过多种方式感知环境的变化，如网络带宽的变化，系统负载的变化，用户访问习惯的改变等；并且通过不断的收集这些信息，在智能分析后提取出有用的知识，以便调整系统，提高服务效率。

- 自传播和自复制的能力

系统中的资源具有自我传播和自我复制的能力。系统通过收集用户访问习惯，系统负载变化和网络带宽变化等信息后，能够将资源迁移到最靠近用户的地方，或者为资源建立多个副本，以满足用户访问速度和可用性的需要。

- 自我免疫能力

系统具有良好的免疫能力，可以模仿生物体抵御病菌侵袭的免疫系统的免疫机制，以实现能自主检测入侵、自主抗攻击、自主防御和自主恢复的自主抗毁结构。这种能力使系统具有良好的可靠性和可用性。

- 自我进化能力

系统具有良好的进化能力。系统通过不断的自学习和不断的积累知识，能够变得更“聪明”，从而更能有效的调整资源和任务的分布，更好地满足用户需求。

- 自我修复能力

系统在具有良好自我免疫能力的基础上，具有良好的自我修复能力。如果仅仅是信息文件损坏或者丢失，系统可以通过自复制机制重新恢复信息。如果系统中的计算机出现硬件故障，系统能够快速的探测到出现故障的节点，并且将该节点排除出系统，调整信息资源和任务的分配，不中断服务。

- 良好的用户接口

系统提供多种用户接口，包括应用程序函数库，系统管理界面，能够满足现有不同用户的需要，保证用户有效的利用信息资源。

- 良好的性价比

系统大量采用具有最好性价比的普通服务器，降低了对昂贵的大型机的依赖。系统大量采用由计算机直接管理的普通 SCSI 或者 SATA 硬盘组成分布式并行的存储系统，不需昂贵的 SAN 或者 NAS 存储系统，从而有效的降低了存储系统的资金开销。

- 分布性

系统不是集中地驻留在某个节点上，而且也不是集中部署于一个地方，而是由分布于许多地方的大量计算机构成。这样的部署方式有效的适应了用户分布于各地的特点，能够有效的降低对骨干网络的带宽压力，提高对用户请求的响应速度。

- 并行性

系统中各数字有机体站，各节点同时为用户提供服务，无主从之分。各数字有机体站既可独立提供服务，也可以协同提供服务，从而突破了传统系统的网络 IO 瓶颈。系统具有性能优良的调度系统，能够实现全系统负载均衡，从而提高系统的资源利用率和数据吞吐率。

- 透明性

系统能很好地隐藏系统内部的实现细节。如资源的物理位置、并发控制、系统故障等对用户都是透明的，使用户感觉整个系统就尤如一台机器一样。例如，当用户要访问某个文件时，只需要提供文件名而无须知道它是驻留在哪个节点上，即可对它进行访问，亦即具有物理位置的透明性。

- 共享性

系统中，分布在各个节点，各数字有机体站的软、硬件资源，可供全系统中的所有用户依照授权进行共享，并能以透明方式对它们进行访问。

6 数字有机体解决方案

6.1 物理部署结构

6.1.1 国家教育信息平台的部署结构

从物理部署结构上讲，本解决方案仍然采用教育部、各省级信息中心和各地市信息中心的多点部署结构。这个结构如图 6-1 所示。

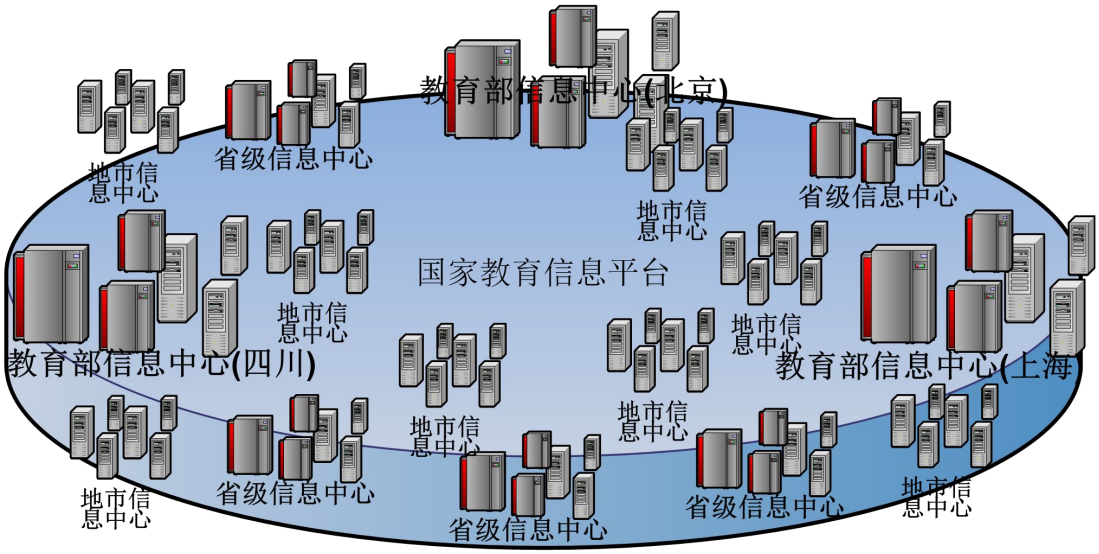

图6-1 国家教育管理信息系统的物理部署整体结构示意图

各个信息中心，尤其是教育部和省级信息中心，将以国家教育科研网为主要互联网络，而以电信、联通、移动等的网络为辅助互联网络。各地市的信息中心，建议尽量以教育科研网为主，以电信、联通和移动等的网络为辅助。五级教育机构的各个部门，尽量以教育网接入系统，也可以用其他运营商网络接入系统。

从规模大小来看，系统可能存在层次关系。例如，建议建立至少三个规模较大的教育部信息中心，并分别分布在地理位置适中的地方。各省又建立规模适中的信息中心，然后各地市又建立更小的信息中心。但是，这种层级结构只是体现在规模大小上，并不是系统的逻辑结构。

实际上，这些信息中心在逻辑上是平等的，它们共同组织为一个系统。和旧方案不同，系统中的每个信息中心并不是孤立的，也不是一定只为本地区的用户提供服务。在这个系统中，所有的信息中心，将在数字有机体系统的整合下，共同向所有的用户提供服务，从而形成一个真正意义上的公共服务平台。每个信息中心，基于就近服务的原则，将主要为本地区的用户提供服务。但是，在其他信

息中心负载过重，或者其他信息中心故障的时候，它也将自动为其他地区的用户提供服务。

同时，系统中各个存储设备也不是单独使用的，而是在数字有机体大规模存储系统的整合下，形成一个公共的存储池，各种应用都将使用这个存储池来存储数据。本解决方案也不建议采用昂贵的网络存储系统。本解决方案建议采用廉价的主机附接存储或者磁盘阵列来构建共享存储系统。

在实际应用时，可以根据教育部组织结构的层次关系，形成相应的层级服务关系。这时，分布在多省的各个教育部信息中心共同承载教育部自身的业务，满足教育部自有业务的服务需求、存储需求和抗毁容灾需求等。同时，这些信息中心也用于为全国各个区域的省级教育机构提供就近的教育部服务。甚至可将教育部的服务分布到每个省级中心，从而就近为各省提供教育部的服务。对于这个服务层次，我们称为部级教育信息服务。

在各个省内，教育厅都可以向本省的教育机构提供特有的教育服务。这些服务将由部署在省教育厅和各地市教育主管机关的信息中心内，共同向全省提供教育服务。我们将这个层次的服务称为省级教育信息服务。

类似的，根据教育机构的组织关系，还可形成更低层级的服务网络。但是，从建设成本考虑，建议先建立部级教育信息服务网络，然后再根据业务发展的需求逐步建立省市的教育服务网络等。

在这个部署结构上，将通过数字有机体系统实现抗毁容灾，分散网络流量，均衡业务负载，提升服务效果，增强系统扩展性和承载各种应用业务的目标。

6.1.2 单个信息中心的部署结构

在一个信息中心内，主要设备的部署结构如图 6-2 所示。整个数据中心从网络结构上可以划分为网络接入区、外网服务区、内网服务区、系统管理区和内部办公终端区。

6.1.2.1网络接入区

网络接入区以接入防火墙为界，一直到连入互联网络的区域都是网络接入区。网络接入区设备部署的主要目的是：

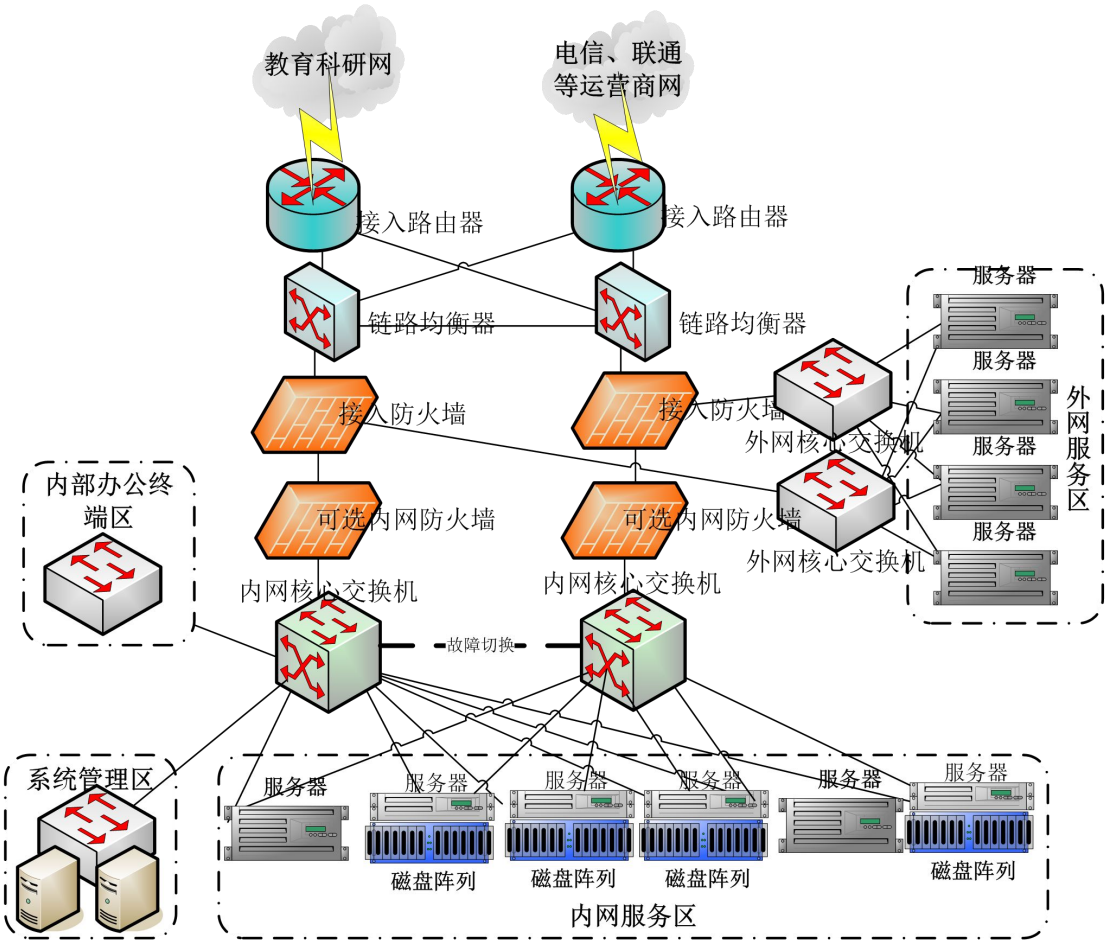

图6-2 单一信息中心的内部物理结构示意图

1）多链路接入，达到流量均衡和容灾

这部分主要由接入链路、接入路由器和链路均衡器完成。一个信息中心需要为全省，甚至外省的用户提供服务。这些用户可能来自教育网、电信网、联通网等。在中国这种各个运营商网络条块分割的情况下，只接入单个运营商网络难以满足各种用户的需求。因此需要同时接入多个运营商的网络。同时，从链路容灾考虑，只有一个运营商的链路也是不可靠的。

在本解决方案下，各个信息中心之间也存在着一定的网络流量。这个流量不是汇聚型的，而是每个信息中心都需要和其他各个信息中心通信。这些通信包括很小流量的系统管理通信、较大流量的数据复制通信、以及业务迁移通信等。这些通信建议以教育科研网为主要通信渠道（理由是教育科研网本身是教育部的，可以更低的费用获得较大的带宽）。在教育科研网故障时才选择其他运营商链路。其他运营商链路主要用于用户接入。因此，要求链路流量均衡器能够根据目标地址进行分流。

2）接入安全

通常，在网络接入区将部署一些网络接入安全产品，例如防火墙、防病毒网

关、网络入侵检测、网络安全审计等设备，以保护外网服务区的安全。

建议根据实际需要部署这些接入安全设备。

3）网络冗余部署

考虑到单一设备本身不够可靠，建议采用双设备冗余部署方式。这样，接入安全设备、链路均衡器、防火墙、内网核心交换机、外网核心交换机等都将采用热备份方式，从而达到网络冗余部署的目标。

6.1.2.2外网服务区

外网服务区用于部署对外提供服务的服务器群。对外网服务区的服务器，接入防火墙允许外部用户访问它，而不允许服务器主动访问外部用户。

外网服务区的服务器本身并不存储任何业务数据，也不执行任何业务逻辑。其任务仅仅是提供静态数据、数据显示、请求接受和响应。业务逻辑执行和业务数据存储将在内网服务器上完成。从而使得攻击者即使攻破外网防火墙及其主机系统，也不至于造成严重的破坏。

外网服务区将根据需要部署几台到几十台服务器。服务器间通过数字有机体系统实现负载均衡。系统需要对外提供服务的业务将按照需要部署在这些服务器上。一个业务可能同时部署在多台物理服务器上，这将由系统根据需要自动调度。在某台物理服务器故障，或者某台物理服务器上的业务故障时，其他物理服务器上的业务服务器将继续提供服务，并且可以在新的物理服务器上启动业务服务，从而满足业务容灾、服务能力和负载均衡等需求。因此，本解决方案不需要部署单独的，昂贵的网络负载均衡器。而且能够更好的均衡物理主机的负载，达到更好的服务效果和资源利用率。

6.1.2.3内网服务区

1）网络结构

在内网核心交换机和接入防火墙间可以再部署一台异构的内网防火墙，以增强内网的安全性。如果资金紧张，也可以不部署，而由接入防火墙限制互联网用户不可访问内网即可。

内网服务区用于部署提供内部业务和提供外网业务服务以及数据存储服务的服务器。这些服务器通过接入防火墙和可选内网防火墙的保护，可以防止互联网用户直接访问它们。

2）存储

根据信息中心的规模，内网服务区将部署几台到上百台服务器。这些服务器可以具有不同的性能，可以是新旧不同的，也可以外接容量不同的存储设备。建议这些服务器至少是 PC 服务器以上等级的。每台服务器除了系统硬盘外，建议内置一定容量的数据磁盘，也可以外接磁盘阵列，以扩展服务器的存储能力。服务器的计算能力、内存容量和磁盘存储系统的性能最好相互适应。

在内网服务区，无需部署价格昂贵的 SAN 存储系统。考虑到系统需要海量存储空间，建议采用可以内置 12 块以上硬盘的服务器，并外接一台高性价比的磁盘阵列。这样，每台服务器可以获得数十到近百 TB 的存储容量。在数字有机体大规模存储系统的整合下，所有服务器的存储将整合在一起，从而满足海量数据存储的需求。这个存储系统也很容易扩展。它可以通过为服务器增加存储设备、增加服务器等方式扩展容量。单个信息中心的存储容量可以轻松的扩展到数 PB。

3）服务器组织

内网服务区的服务器并不需要划分为数据库服务器、应用服务器、中间件服务器、备份服务器等不同的类型，而是统一整合为一个服务系统。在数字有机体系统中，每台服务器既是数据库服务器，也是应用服务器，也是备份服务器。数字有机体系统不建议采用中间件，除非有特别需要（因为大多数中间件的功能都由数字有机体系统自身实现了，例如通信中间件、存储访问中间件等）。考虑到业务的处理都是需要业务数据支撑的，如果业务数据和业务处理分布在不同的服务器上，则数据的访问必然出现瓶颈。因此，数字有机体系统将数据分散存储到服务器中，并智能的进行复制，从而既解决了数据访问效率问题，也实现了数据抗毁容灾的功能。当然，可以从任何一台服务器上进行数据离线备份，例如备份到磁带系统或者光盘中。如果你固定选择一台，那它就是你的离线备份服务器。

这样，外网服务器在请求执行业务逻辑时，将由数字有机体系统自动调度到内网的某台服务器上完成，无需再使用实现负载均衡的中间件等。

4）数据库服务

数字有机体系统包含数字有机体数据库系统。他是能够处理海量记录、数据智能复制（含异地复制）、提供大数据查询服务的数据库系统。通常，它和数字有机体系统一起部署，无需单独的服务器。当然，出于特殊的考虑，也可以部署专门的数字有机体数据库服务系统（由分散部署在多地的，数量根据需要决定的服务器构成）。根据教育管理系统的需求，建议不专门部署这样的系统。数字有机体数据库系统已经具有本地和异地复制功能，因此也无需专门的数据库备份系统和容灾系统。

6.1.2.4系统管理区和内部办公终端区

系统管理区将部署系统管理服务器及其管理工作站。如果需要，也可以建立专门的管理中心，采用电视墙和大屏等方式对系统运行状态进行实时监控。系统管理区的建设具体参见“运维系统”这一章节。

信息中心对应的教育主管机构的办公区将在内部办公终端区中，通过内网核心交换机接入系统，完成内部办公。必要时，可以建立独立的连接外网的外网办公区，用于访问上级教育部门的系统。

6.2 软件逻辑结构

本解决方案采用层次型的软件结构，支持多种业务运行方式，提供各种应用支撑服务，完全满足各种业务系统的运行需求。

6.2.1 软件层次结构

本解决方案的软件层次结构如图 6-3 所示。它采用系统平台层、应用支撑层和应用层这样的层次结构。

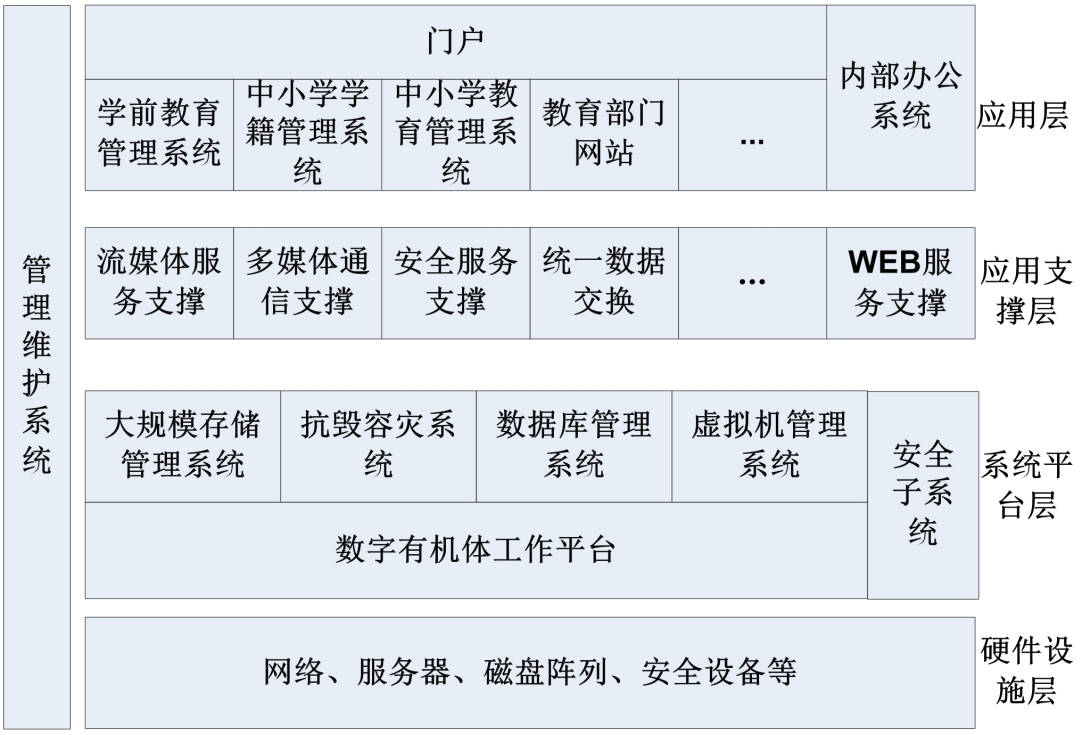

图 6-3 系统软件层次结构

系统平台层主要由数字有机体系统构成，包括数字有机体系统的工作平台、

大规模存储管理系统、抗毁容灾系统、数字有机体工作库、虚拟机管理系统和安全子系统等。这些系统的具体介绍请参见 5.2 节“基础平台简介”部分。

应用支撑层由各种应用支撑软件构成。流媒体服务支撑由数字有机体流媒体服务子系统提供。它能够提供流媒体点播服务、转播服务、轮播服务和存储点播服务等，是建立各种流媒体应用的通用支撑平台。

多媒体通信支撑可由数字有机体会议系统提供。它能够提供文字、图片、语音、视频等通信手段，具有个人通信、多点会议、好友管理、组织结构管理、会议管理等功能，为建立各类交流系统提供丰富的支持。

安全服务支撑包括统一认证系统、密钥管理服务系统、数字签名及认证系统、文件加密存储系统，以及通信加密传输等。具体的内容参见“安全框架”章节。

统一数据交换平台用于实现各个业务系统之间数据交换。该数据交换平台将根据教育部的数据交换规范实现。

教育管理系统的大多数业务都采取 WEB 服务方式向用户提供。因此，需要构建专门的 WEB 服务支撑子系统。这个系统向各种 WEB 应用服务提供 J2EE 运行环境，支持 WEB 业务的各种特殊分布式需求。具体参见“WEB 服务支撑”章节。

在应用支撑层上可以构建各种业务系统，以满足教育管理的各种需要。这些业务系统可以采用两种不同的运行方式，具体参见“两种业务运行方式”章节。像桌面云这样的应用服务也可以提供。不过，从服务效率等考虑，建议更多采用 WEB 桌面这样的业务形式。

6.2.2 两种业务运行方式

数字有机体系统提供两种业务运行方式，即“沙箱”运行方式和虚拟机运行方式。

采用“沙箱”运行方式的逻辑概念如图 6-4 所示。这时，业务软件必须是一个可以在 Linux 系统下运行的应用软件。它将运行在由数字有机体操作系统安全机制建立的软件“沙箱”环境下，并直接从数字有机体系统获得各种系统级的支撑。这些系统支撑包括通过 Linux 标准文件系统访问数字有机体文件系统，获得工作平台提供的负载均衡服务、抗毁容灾子系统的数据和业务抗毁服务等。因此，从运行效率上讲，该种方式具有最好的运行效率。建议新开发的业务或者已有的 Linux 应用都采用这种方式运行。

图 6-4 数字有机体系统的“沙箱”运行模式

数字有机体系统也提供虚拟机运行方式。其概念结构如图 6-5 所示。这时，每个业务将运行在一个独立的虚拟机内。虚拟机内再安装业务需要的操作系统和相应软件。数字有机体系统通过虚拟机管理系统实现对这些虚拟机的管理。

图 6-5 虚拟机运行模式的逻辑结构

数字有机体系统的虚拟机管理系统提供各种虚拟机管理功能。镜像管理功能

实现虚拟机镜像文件存储管理。虚拟机的镜像文件将被存储到大规模存储管理系统中，通过抗毁容灾子系统实现本地和异地的复制，确保虚拟机镜像文件不损坏和丢失。同时，通过大规模存储管理系统，本地和异地的服务器可以方便地共享虚拟机的镜像文件，以便快速地在不同的服务器上启动虚拟机。运行调度和运行监控系统将管理各个虚拟机的启动、运行和终止。用户管理系统将管理系统用户，认证用户并在用户创建、启动和终止虚拟机时验证权限。自动化服务模块将提供操作系统自动安装，镜像自动离线备份等功能。管理 WEB 服务则是数字有机体虚拟机管理系统的 WEB 门户，以便虚拟机管理人员能够高效的部署和管理各个虚拟机。

和“沙箱”运行模式不同，即使虚拟机内运行的是数字有机体系统，也不能直接访问物理机上运行的数字有机体系统提供的服务。如果他要访问大规模存储管理系统中的数字有机体文件系统，则必须再通过 Windows 操作系统 CIFS 或者 Unix 操作系统的 Samba 客户端。工作平台提供的负载均衡等服务也无法在多个虚拟机间应用。业务抗毁支持只能通过虚拟机运行监控和运行调度在其他物理服务器上启动虚拟机的方式实现。数据库服务则可以通过数据库管理系统的网络服务获得。

根据上述分析，再加上 Windows 操作系统和 oracle 数据库等的安全问题，本解决方案建议只在原有业务系统不需要考虑安全，而且难以移植的情况下，才采用虚拟机运行模式，其他新开发的，可以移植的业务系统，都采用“沙箱”运行模式。

6.2.3 流媒体服务和多媒体通信支撑

数字有机体流媒体系统和多媒体会议系统可以为应用提供各种流媒体服务和多媒体通信服务。

数字有机体流媒体系统采用数字有机体的架构，支持大规模分布式部署，满足高并发，巨大流量的媒体服务需求。它提供常见的视频点播服务，可用于实现类似教学视频点播等业务。它提供录播服务，可用于对教学现场进行录像，并同步播送到远地教学场所。它提供完整的视频监控系统，可用于对教学场所进行全面的视频监控，远程教学监督，远程教学评估等。它提供转播服务，可帮助 IP 组播穿透运营商网络，实现远程校园的多点 IP 组播。它也提供延时续播服务，可以使得直播能够暂停，并在任意时刻继续播放。因此，数字有机体流媒体服务系统可以为教育管理的各种业务提供各种流媒体服务支撑。

数字有机体会议系统具有丰富的多媒体通信功能。它提供个人通信通常需要的人员查询、好友管理、在线消息、离线消息、在线文件传输、离线文件传输、

表情符号，图片粘贴发送、语音电话、视频电话、本地视频播放、PPT 展示等功能，可以作为教育机构工作人员相互通信的工具。它也具有群组通信，按照组织结构显示用户，在组织结构上进行多媒体通话等功能，因此也可以作为教育机构的日常办公通信工具。最重要的是，它具有完善的会议功能，支持会议安排，参会邀请、主席控制、PPT 演示、视频播放等，具有自由设定视频和音频合成的功能，能够和其他会议系统互联互通，因此可以作为教育机构的内部会议系统使用。综上所述，数字有机体会议系统可以为教育管理的各种业务提供丰富的多媒体通信支撑。

6.2.4 WEB 服务支撑

本解决方案尽量利用开放源代码或者国产软件构建 WEB 服务支撑平台，从而使得 WEB 服务能够构建在一个安全的环境下。因此，本解决方案提供的 WEB 服务支撑框架如图 6-6 所示。

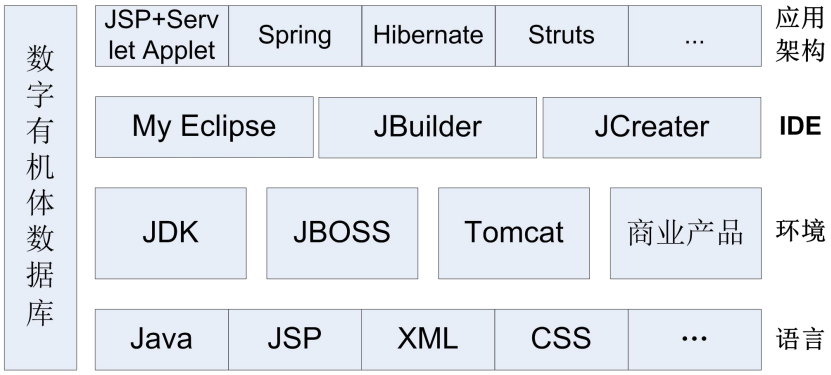

图 6-6 WEB 服务支撑框架

此框架提供了丰富的语言支持，能够适应不同技术背景的开发人员；具有多种可选的 J2EE 环境，便于满足不同需求和规模的业务系统；提供多种集成开发环境，便于开发人员选择熟悉的开发工具，可以采用各种不同的，流行的应用架构，用于满足各种应用需求。因此，本解决方案能够提供足够的 WEB 支撑。如果一定要选择像 WebLogic 等国外产品，本解决方案也是支持的。

6.3 安全框架

6.3.1 安全体系概述

本章节并不讨论安全框架下的系统可靠性这个内容。系统可靠性内容请参见 6.5.3“全面实现抗毁容灾”章节的介绍。

本解决方案的安全框架如图 6-7 所示。其中，物理安全、网络安全、应用安全、安全交付、安全管理、漏洞评估与扫描、信息安全标准规范和条例的内容、实施方案等在许多解决方案中都能找到，而且原解决方案已经进行了充分的论述。本解决方案就不再这些方面进行描述。

图 6-7 安全体系示意图

本安全框架的不同点在于强调操作系统安全、数据库安全和平台安全在安全技术和服务体系中的重要性，并论述数字有机体系统在这三个方面的特有支撑。

6.3.2 数字有机体操作系统安全

数字有机体操作系统基于开放源代码的 Linux 操作系统开发，不仅充分利用了 Linux 系统已有的各种安全手段，还在许多方面提升了操作系统的安全，并针对大规模分布式系统的需要进行了安全增强，是具有自主知识产权的国产化产品。因此，无需担心操作系统存在安全后门，也无需担心技术被外国公司控制。

数字有机体系统充分利用了 Linux 已有的安全机制。这些安全机制包含且不仅包含自主访问控制、PAM、SELinux、IP-TABLES、LIDS、Snort、Snort-Center、

主机安全审计、密钥管理服务和本地加密文件系统等。这些机制使得 Linux 成为一个较为安全的操作系统。

在现有 Linux 操作系统的基础上，数字有机体系统还在以下方面增强了操作系统的安全：

(1) 统一 SELinux：在大规模分布式部署数字有机体系统的情况下，本功能能够保证所有服务器采用协调一致的强制访问控制策略，以防某台服务器脱离系统控制。

(2) 最小特权集：数字有机体系统将超级用户的特权拆分为多个子集，分别赋给不同的管理员。因此，系统不再存在超级管理员。这可防止某人权限过大而对系统造成破坏。

(3) 可信通路：可信通路即为用户提供一个可信的方式登录系统。它预定义了一组键序列，当用户键入这组可信通路序列键后，控制权总是交给操作系统的可信计算基(TCB)，即核心。系统杀死当前所有的用户进程，重新回到登录界面。

(4) 强化身份鉴别：在 Linux 原有 PAM 的基础上，增加了指纹识别、文字笔迹识别等支持，从而强化了系统的身份鉴别能力。

(5) 增强密钥管理服务：利用数字有机体系统的大量服务器分布在多地的特性，将托管的密钥进行特殊存储，使得即使某些节点被攻破，攻击者也无法获得完整的密钥，更无法进行篡改。

(6) 统一身份鉴别和授权系统：建立了独立于 Linux 操作系统的，利用增强密钥管理服务实现的身份鉴别系统。该系统不仅可以用于鉴别系统的用户，也可以用于各个应用程序鉴别自己的用户。同样，利用数字有机体系统的分布式特性，也建立了独立的授权信息存储系统，并利用它实现了独立与 Linux 操作系统的文件访问控制机制。这样，即使是服务器上的特殊用户，也无法越权访问数字有机体存储系统中的文件。

(7) 强化主机身份鉴别：数字有机体系统和云平台一样，由大量服务器构成，如何防止攻击者冒充系统主机，或者进行 IP 伪装等也是重要问题。数字有机体系统具有独立的强化主机身份鉴别机制，可以解决该类问题。

(8) 主机间安全通信：数字有机体系统中的所有服务器间采用特殊的安全通信机制，确保通信安全。

综上所述，数字有机体系统不仅是国产化的操作系统，而且其安全能力也高于开放源代码的 Linux 操作系统。因此，它完全可以为国家教育管理信息系统提供坚实的安全保障。有了操作系统的安全，才能谈得上数据库安全以及应用安全等。

6.3.3 数字有机体数据库安全

数字有机体数据库系统基于开放源代码的 MySQL 数据库开发，并且完全改造了事务执行引擎，使其成为一个具有自主知识产权的产品，因此可以确保其不存在任何安全后门。

除了 MySQL 已有的安全机制，如用户登录认证、访问控制机制外，数字有机体系统还针对大规模分布式部署的需要，增加了以下安全支持：

(1) 主机身份鉴别：对加入系统的服务器进行强制身份鉴别，并在每次通信时进行身份确认，以防止攻击者冒充系统节点，或者假冒系统节点的 IP 来发送攻击信息。

(2) 主机间加密通信：所有主机间通信采用动态加密，防止攻击者窃取信息。

(3) 分布式访问审计：针对数字有机体系统中客户可以同时访问系统多个节点的问题，设计了分布式访问审计系统，以尽快发现可能的攻击行为。

数字有机体系统还可以为数据库提供数据加密服务、数据文件强制访问控制支持，以及增强的密钥管理服务等，从而使得数字有机体的数据库安全特性进一步增强。

6.3.4 数字有机体平台安全

数字有机体系统提供两种业务运行方式，即“沙箱”模式和虚拟机模式。两种模式都能提供良好的业务隔离能力，能确保各个业务系统的数据、进程、运行信息等相互不可见，从而使得业务能够安全可靠地运行在各自独立的环境下。

数字有机体平台提供两种 PKI 基础设施部署模式。一种模式采用堡垒主机，即将 PKI 基础设施部署在特殊的，经过安全加固，并用专门防火墙保护的服务器上，以增强 PKI 基础设施本身的安全性。另一种模式采用数字有机体系统提供的加密文件系统和增强的密钥管理服务来保存 PKI 认证信息，并将 PKI 服务软件部署在数字有机体服务器上。后一种模式增强了 PKI 基础实施的可靠性，并且认证信息分布式加密存储，提升了认证信息的安全性。两种模式都能向平台及上层的应用提供统一的数字认证和数字签名及鉴别服务，支持 CA 和 RA 分开部署，满足建立教育系统认证体系的需求。

数字有机体系统在开源代码的基础上研发出完整的平台系统，整个体系具有自主知识产权，完全掌握整个系统的源代码，因此不存在任何安全后门，也无需受制于国外公司。

6.4 运维管理系统

数字有机体系统具备完善的运维管理信息系统，该信息系统的框架如图 6-8 所示。数字有机体运维管理平台将信息采集器分布到系统的每一个角落，实时获取系统的运行状态，尤其是报警信息，实时地通过统一报警平台向相关人员报警；并以运维管理门户为入口，向各级管理人员提供系统的实时图形化的运行状态、历史数据分析以及趋势预测等。

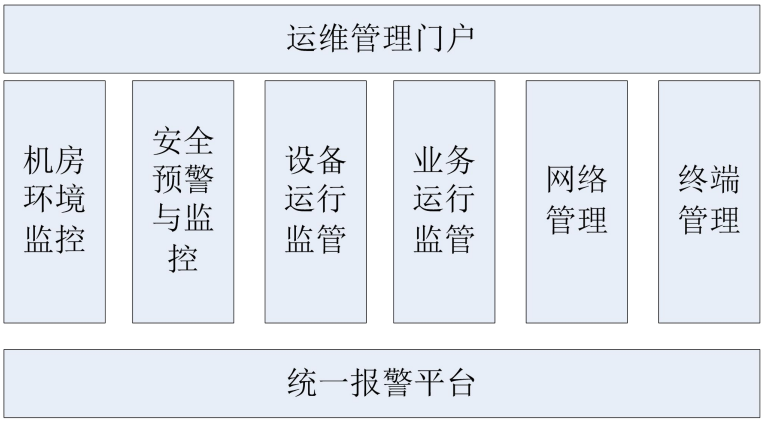

图 6-8 运维管理信息系统结构

数字有机体运维管理平台通过统一报警平台向各级管理员及时报警，支持的报警手段包括：

(1) 在线图形化显示；
(2) 管理终端声音警示；
(3) 数字有机体会议系统短消息报警；
(4) 外接警报装置报警；
(5) 通过电信网关手机短信报警；
(6) 通过电信网关自动拨号报警等。

数字有机体运维管理平台通过运维管理门户网站向各级管理员提供图形化的实时管理界面。该管理门户支持的功能有：

(1) 电子地图上各信息中心运行状态图形化显示；
(2) 各级电子地图跳转、放大、缩小等功能；
(3) 各子系统电子地图上实时显示运行状态；
(4) 报警和运行日志信息实时刷新；
(5) 监控对象实时曲线图；
(6) 历史数据统计图；

(7) 历史数据自定义统计分析；
(8) 数据变化趋势预测；
(9) 管理日志记录；
(10) 故障处理跟踪；
(11) 外包服务跟踪。

数字有机体运维管理平台可以管理到系统的各个方面。各大模块的管理对象分别如下。

(1) 机房环境监控模块用于监控系统的物理运行环境，可以监控：温度、湿度、二氧化碳浓度、粉尘数、电路电压、浸水、烟雾等。
(2) 安全预警与监控系统的采集器针对各种安全设备，可以监控防火墙、入侵检测、防病毒、网络安全审计、服务器的主机防火墙、主机入侵检测、主机安全审计、路由器和交换机的网络安全报警等。
(3) 设备运行状态监管模块可以实时监控：服务器的 CPU、内存、网络、磁盘 I/O 等负载信息，主要进程运行状态，服务器的 CPU 温度、机箱温度、主板电压、CPU 电压、机箱风扇、CPU 风扇等的运行状况.
(4) 业务运行监管可以监控：业务进程状态、业务虚拟机状态、业务使用带宽等。在业务模块的配合下，还可以收集业务在线用户信息和运行日志等。
(5) 网络管理模块用于监管网络设备，支持的设备包括路由器、智能交换机、防火墙、可管理网关等。能够采集设备的负载状况，链路流量信息、端口状态信息、运行日志信息、报警信息等，
(6) 终端管理模块用于管理办公终端和管理终端等。通过驻留在终端上的信息收集器，可以收集每个终端的登录信息、负载信息、网络访问信息、文件操作信息、外设使用信息、程序运行信息等。

数字有机体运维管理平台充分考虑了现实环境中常见的多级管理模式。可根据系统的部署状况，建立信息中心间的层级关系。每级信息中心的管理人员可以管理到自身信息中心以及下面各级信息中心的各个子系统。因此，可以由上级信息中心代管下级信息中心，下级信息中心只需一两个配合人员即可。这种集中管理模式可有效减少基层信息中心的人力开销。

其他有关制度建设、工作流程建设、管理队伍建设等内容在原有解决方案中已经详细描述，本解决方案不再论述。

6.5 其他主要目标的实现

在“安全框架”章节已经描述了实现共享安全服务平台的方式。在“运维管理系统”章节介绍了建立高效运行维护系统的方式。在“两种业务运行方式”章节已经说明了建立共享的业务运行平台的方式。下面将描述其他主要需求和建设目标在本解决方案中的实现方式。

6.5.1 满足国家教育管理信息系统部署和服务的需要

根据国家教育管理信息系统的逻辑结构，本解决方案建议采取以下部署方式：

(1) 国家信息系统面向全国教育机构，因此同时部署在教育部的信息中心（至少三个）和各省的信息中心。在每个信息中心内部，采用“沙箱”运行方式，同时运行在多台外网服务器，并由数字有机体系统实现负载均衡。在多台内网服务器上以“沙箱”模式部署业务逻辑服务程序，并将数据存储在数字有机体数据库和文件系统中，由系统自动实现负载均衡。信息中心之间的负载均衡由数字有机体系统的全局调度系统实现，并达到就近服务的目的。

(2) 教育部自有的业务中，可以移植到数字有机体系统上的业务和新开发业务采用“沙箱”模式运行在教育部的信息中心；由系统自动实现负载均衡。无法移植到数字有机体系统的业务采用“虚拟机”模式运行在教育部的本地信息中心。

(3) 各省教育机构的自有业务系统中，可以移植到数字有机体系统上的业务和新开发业务采用“沙箱”模式运行在各自的信息中心中。如果需要面向全省各地市服务，也可以采用类似国家信息系统的运行方式，扩展运行到各个地市的信息中心中。无法移植到数字有机体系统上的业务采用“虚拟机”模式运行在本地的信息中心中。

6.5.2 建设集中统一的教育基础数据库

考虑到全国学生的数量庞大，如果采用单一存储系统单一数据库来实现，必然需要昂贵的存储设备、小型机甚至大型机（或者服务器集群），以及昂贵的oracle数据库。因此，本解决方案建议建设虚拟集中统一的教育基础数据库。

首先，教育基础数据库将分为学生、教师、学校资产及办学条件三大类基础

数据库。每类基础数据库再根据业务系统划分为多个更小的业务数据库。所有业务数据库采用同一套信息与数据标准规范，以确保各个业务数据库间相同数据具有同样的语义和格式，能够相互交换。

对每个业务数据库，分为两级逻辑子库，即国家级业务数据库和省级业务数据库。国家级业务数据库物理存储在国家级信息中心（即教育部信息中心），各省级业务数据库分别存储在本省的信息中心，然后按照异地容灾的要求进行复制。省以下，如地市、县和学校三级基础数据库，建议根据数据量决定是否进一步划分。通常一个表的数据量在一千万条以下都是数字有机体数据库能够承载的。如果不划分，地市、县和学校三级的基础数据库实际上仅仅是省级数据库中的一个子表。

这样，整个教育基础数据库将被划分为数百个逻辑数据库。这些逻辑数据库分别存储在不同的信息中心。数字有机体系统能够将其整合为一个虚拟数据库，即系统中的任意一台服务器都可根据授权访问每个逻辑数据库。这样，数据交换平台软件可以运行在教育部和各省信息中心的服务器上，通过数字有机体系统的数据库共享机制，实现数据交换。

数字有机体系统采用分布式策略存储这些逻辑数据库，他们将分散存储在许多服务器上。因此，无需购买昂贵的网络存储设备，可以用高性价比的磁盘阵列来存储这些逻辑数据库。这些服务器共同提供数据库服务，因此无需购买昂贵的小型机等，可以采用较高性能的通用服务器。

6.5.3 实现全面抗毁容灾

在本解决方案中，数字有机体系统提供了天然的抗毁容灾实现，可以全面地实现数据、业务和系统的抗毁容灾。在系统层面，当某些信息中心故障时，数字有机体系统能够重新组织系统结构，并调整数据，业务的分布，继续提供降级后的服务，使整个系统不至奔溃。

6.5.3.1数据抗毁容灾

数字有机体系统具有完整的文件和数据库的本地和异地复制。文件数据的抗毁容灾具有如下功能：

(1) 支持本地复制和异地复制；

(2) 支持系统自动决定异地副本位置或者指定异地副本位置；

(3) 支持不大于 10 个的任意副本数复制；

(4) 支持同步复制和异步复制；

(5) 支持最少副本同步更新机制，余下未同步更新副本将异步更新；
(6) 采用操作日志同步方式，无需完整复制；
(7) 自动检测副本是否损坏，被损坏的副本自动恢复；
(8) 根据副本丢失和恢复状况自动增减副本；
(9) 根据文件访问状况合理迁移或者增加副本；
(10) 支持多副本并发读取。

数据库系统的抗毁容灾功能如下：
(1) 支持本地复制和异地复制；
(2) 支持系统自动决定异地副本位置或者指定异地副本位置；
(3) 支持不大于 5 个的任意副本数复制；
(4) 支持同步复制和异步复制；
(5) 支持分布式事务，支持多机并发访问；
(6) 采用混合日志同步，减少传递数据量；
(7) 自动根据副本丢失状况增加副本。

数字有机体文件系统和数据库系统都支持本地复制和异地复制，都支持指定异地复制位置。根据教育管理部门的组织结构和信息中心的规模状况，建议采用如下的复制策略：

(1) 若本级信息中心没有建设其他相当规模的异地信息中心，则将数据复制到上级信息中心；如本级信息中心建设有相当规模的异地信息中心，则复制到异地信息中心。
(2) 根据数据的可靠性需求，对需要高可用的数据采用同步异地复制策略，对可用性要求不是很高的数据采用异步异地复制策略，普通数据只在本地进行复制。
(3) 教育部的核心数据同步复制到至少三个教育部信息中心；较高可用性需求的数据由系统自动复制到一个异地信息中心。
(4) 建立离线备份机制，各个数据中心将自己的数据备份到本地的磁带存储系统中。

这样，系统中的重要数据既有本地复制又有异地在线复制，而且还有离线备份。在本地存储系统完全崩溃时，业务系统可从异地复制获取数据进行服务，而且系统将自动增加副本，确保数据的可用性。同时，即使整个系统都被摧毁，也可以从离线备份进行恢复。因此本解决方案已经提供了足够的数据高可用性保障。

6.5.3.2业务抗毁容灾

数字有机体系统为业务抗毁容灾提供了以下支持：

(1) 通过数字有机体文件系统，运行在各个信息中心服务器上的业务程序可共享同一个文件系统，从而解决了普通共享存储设备难以支持多地并发访问的问题，使业务需要的文件数据可以随时随地获得；

(2) 通过数字有机体数据库系统，运行在各个信息中心服务器上的业务程序可共享同一个分布式数据库；

(3) 数据抗毁容灾使得一个信息中心被摧毁后，业务迁移到其他信息中心后仍然可以获得需要的数据；

(4) 提供虚拟机状态监控和自动恢复功能。在发现业务运行的虚拟机死亡后，自动在其他服务器或者异地的服务器上启动业务虚拟机，继续进行服务。

(5) 各个信息中心间互联互通，并且由数字有机体系统进行统一管理调度，业务系统可以同时运行在各个信息中心，形成自然的抗毁容灾结构。

(6) 对运行在“沙箱”内的业务系统，提供全局负载均衡（含信息中心内负载均衡，多信息中心负载均衡和就近服务），故障服务器自动屏蔽，以及自动选择物理服务器启动业务系统，从而使得业务系统在遭遇各种故障时仍然能够继续提供服务；

(7) 对运行在“沙箱”内的业务系统，可实现会话信息同步复制，在某台服务器故障时，正在进行的会话可迁移到复制服务器上，保持会话继续进行，达到从“断点”恢复的目的。

综上所述，本解决方案建议采取如下的业务容灾策略：

(1) 由于各个信息中心都可作为其他信息中心的冗余备份，因此系统的总体冗余可以小于 1。根据实际经验，系统服务能力冗余量为 0.6 即可。

(2) 无需单独建设备份中心，也无需单独建设数据容灾系统。

(3) 配置各个信息中心各个业务的容灾策略。对需要满足各地服务需求的业务，直接采用多信息中心并行服务的方式（各信息中心内部又可采用多机并行服务方式）。对只需为本信息中心用户提供服务的业务，采取本信息中心多机并行服务方式，并配置多个备份异地信息中心，或者由系统自动选择。对只需单虚拟机运行的业务，配置可迁移服务器和信息中心，或者由系统自动选择。对无需抗毁容灾的服务，禁止系统自动容灾。

6.5.4 满足系统不断扩展的需要

本解决方案具有全面的扩展能力，网络、存储和服务能力都能方便地进行扩展。

本解决方案支持多信息中心并行提供服务，而且按照就近服务的原则分散网络流量。因此，在单个信息中心无法获得足够网络带宽时，可以增建信息中心来分担网络流量。更重要的是：增建的信息中心将和原有信息中心融合为一个整体，在业务逻辑上完全融合，无需修改业务程序。

如前所述，数字有机体系统能够整合各个信息中心的所有服务器附接的存储系统，形成一个虚拟的存储池，以便各个业务系统共享存储设备，共享数据信息。这个系统可以通过扩展单台服务器的存储系统、增加某个信息中心的服务器，乃至增建信息中心的方式扩展存储空间，提升存储访问带宽，而不受限于任何单一设备。新增加的存储设备可以在线融入存储池，无需停机升级。

如前所述，数字有机体系统支持大规模分布式并行服务。对一个业务系统来说，可以同时运行在多个信息中心的大量服务器上。数字有机体系统自动实现全局负载均衡，就近服务和本地负载均衡，无需部署物理负载均衡器，也不受单个数据中心的网络带宽、服务器数量等限制。因此，本解决方案能够通过增加运行业务的服务器和增加运行业务的信息中心来提高单一业务系统的服务能力。对于面向全国的信息管理系统，例如中小学学籍管理系统来说，这种能够在就近的省级信息中心提供服务的能力有效的降低了对教育部信息中心服务规模、网络带宽等的要求。

7 对比分析

下表是对比原有方案和数字有机体方案的情况，从中可以看出，数字有机体方案具有更好的功能和性能，更能满足教育管理信息系统的需求。

表 7-1 两个方案的对比分析

项目	原方案	数字有机体方案
核心技术	基于硬件虚拟化的云平台	分布式并行处理、抗毁容灾、硬件虚拟化、软件即服务、操作系统安全
核心软件	Linux 和 Windows、Oracle 和 SQL Server 数据库、未确定的云平台	数字有机体系统

存储系统	FC-SAN 和光纤带库	由高性价比磁盘阵列构成的虚拟存储池
服务虚拟化	虚拟机	安全“沙箱”和虚拟机
服务技术	应用负载均衡设备+虚拟机集群，各信息中心独自服务	由分布在各信息中心的服务器构成的分布式并行服务系统
服务设备	单机达到 22 万的高端服务器	10 万以下的高性价比服务器
数据备份	本地光纤磁带库	本地和异地智能在线复制，可选本地磁带备份
抗毁容灾	需后期投资，每个信息中心单独建设	融合到解决方案中，具有高抗毁容灾能力
服务带宽	各省的服务带宽受单一数据中心带宽限制	业务分布式部署，各省也可建多个信息中心来提供服务
存储扩展能力	受限于单一存储设备，在数百 TB 左右。	无存储扩展限制
单一业务服务能力	十多台的服务器集群，且受单一应用负载均衡设备能力限制	无限制
安全保障	制度、网络安全设备	独有的操作系统、数据库和平台安全技术
操作系统安全	等待外国公司打补丁	自有知识产权，高安全操作系统
数据库安全	由 Oracle 或者微软负责	自有知识产品，安全数据库
运维信息系统	新开发建设	已有配套的全面的运维信息系统