

某旅游产业云解决方案

1 需求分析

1) 利用已有资源构建统一的基础实施

当前不少旅游景区已经构建了独立的信息化系统，部署了大量网络、服务器和终端。这些设备应当被集成到新的系统中，而不是报废掉。

在全省，各个旅游景区的信息化系统应当构建在一个统一的基础实施上，实现硬件资源的共享和按需分配，实现数据的抗毁容灾，业务的抗毁容灾，以最少的投入，获得性能优良的基础实施，保证各个景区的信息化系统能够满足各种应用需求。

在全省，各个旅游景区的信息化系统需要整合为一个整体，实现信息的流通、共享和全面分析处理，使旅游管理部门能够全面地、实时的、准确的掌握每个景区的状况，分析挖掘全省旅游产业的发展规律、优势项目、旅客来源、潜在增长点，从而为旅游产业发展做出应有的贡献。

2) 旅游联盟化经营需要大型信息平台支撑

旅游业在过去是一种“散、小、弱、差”的局面，近几年，随着竞争的加剧以及人们思维的革新，联盟化经营发展的趋势越来越明显。旅游联盟化带来了新的信息服务需求，综合化、一体化的产品提供需要广覆盖的信息网络来支撑，才能实现信息的快速传递以及共享。

3) 旅游资源的高度共享与利用需要信息科技

通过信息化建设加强了对旅游企业的管理，如旅游行程单管理，通过统一的行程单规范旅行社行程、导游，避免强制消费等现象；实现全市范围资源信息的相互查询、调用功能，形成统一的资源库。

在旅游云建设中，应充分考虑旅游资源的互联互通、协同应用、资源共享等功能，以解决目前旅游资源系统相对分散、存在较多信息孤岛、整合成本高、管理难等问题，从而形成一个一体化、整合性、通用性的旅游资源管理系统，实现所有资源在相互独立的系统下运营的同时，又可相互查询、调用，形成统一的资源管理和数据库。

通过整合旅游服务资源，形成统一旅游信息平台，推进数字景区信息系统和数据库建设，加强旅游信息资源的开发利用，推广虚拟旅游体验、全信息服务自助旅游、旅游网络推介等系统应用，实现全省旅游资源的共享。整合网络服务资源，形成统一旅游服务内容的综合服务应用，推进各种基础功能的集成和业务系统的无缝接入；建好旅游门户网站，推进全市旅游电子商务应用，并充分利用门户网站的宣传作用，推介全省旅游云。

4) 个性化旅游亟需全方位的信息咨询服务

传统的随团旅游，食、住、行、游、娱等内容基本上都是旅行社安排好了的，规模优势明显，价格也相对便宜实惠，但是旅行者不能自主地安排自己的行程，无法更大程度地享受

到旅游的乐趣。

而近年来的游客中，自主的个性化旅游逐渐占居主导地位。个性化旅游带给游客的是全新的旅游体验，游客可以自主安排自己的旅游时间，自己设计旅游线路，自主选择食、宿、娱等内容，进而从中完全享受到旅游的乐趣。

个性化旅游为旅游服务市场带来了新的需求。游客在旅游前需要很好地了解旅游目的地的信息，包括旅游景点的情况、天气情况、人流量情况等等，游客需要这些信息来决策。在到达目的地后，就更需要了解当地的各种信息，这也是游客对旅游信息咨询服务需求最为迫切的部分。来到一个陌生的区域，游客需要对食(特色菜品、消费价位、推荐指数、餐馆位置)、住(宾馆星级、价格、推荐指数、地理位置)、行(自驾行车路线、路况信息、租车)等大量的信息进行全面的了解。

游客多样化、全方位的信息咨询服务需求要求旅游服务提供商拥有强大的资源整合能力，服务商通过把交通、住宿、餐饮、旅游等信息资源整合到一个平台上，使旅游者能够方便、快捷地获取所需的信息。

5) 旅游电子商务呼唤综合服务组合应用

旅游产品是将吃、住、行、游、购、娱等诸多信息组合起来的信息产品，旅游的销售过程实际上就是产品信息的传递过程，信息流和资金流涉及较多，物流很少，这些特征很适合用电子商务的方式去实现。电子商务的低成本、支付电子化、信息高效传递、宣传覆盖面广等特性是传统旅游业所不具备的。旅游电子商务中，售前旅游企业可以借助网上主页和电子邮件在全球范围内进行宣传，客户可借助网上搜索工具快速找到需要的旅游产品信息；售中可以实现网上订购、网上支付，还可以实现旅游产品模拟体验；售后的信息反馈更及时，可以对消费者的行为进行有效分析。因此，旅游电子商务是旅游产业发展的必然趋势。

旅游电子商务的蓬勃发展使得旅游企业的综合化信息服务平台需求强烈。越来越多的旅游电子商务企业兴起，他们的网络建设包括两部分：外部网站建设和内部数据处理系统。外部网站建设包括形象宣传、业务受理接口、信息查询等诸多功能模块。内部数据处理系统包括业务分析处理、内部信息传递网络等等。

2 设计原则

本方案将根据以下设计原则来完成系统的设计。

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、国产化的网络产品、国产化的安全设备等。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。

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。摒弃国外垄断商业集团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。

3) 全面考虑抗毁容灾

全面考虑抗毁容灾，不是分别为每台设备、每个系统建立容灾机制，而是全面的、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。

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不断扩展的应用需求。因此，系统的基础设施必然是分散的、就近部署的。但是，这些分散部署的基础实施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解决方案。

5) 全面考虑系统扩展性

着眼于未来发展，全省旅游产业云需要满足各级旅游管理机构、各个景区不断增长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很强的扩展能力。采取为未来需求预置设备的方式是在浪费资源；充分利用现有设备，并能按需扩展系统能力才是理想的解决办法。

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，减小管理工作量，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。

7) 开放性

平台支持开放的 API，整合各景区现有应用和设备，同时可以接入第三方应用、内容和服务，博取各家之长，共建区域旅游产业资源公共服务云平台。

8) 采用分步式建设，保证良好的兼容性和扩展性

最大限度地保证各景区现有各种计算机软、硬件资源的可用性和连续性，为不同的现存网络提供互联和升级的手段，保证各种在用计算机系统(包括工作站、服务器和微机等设备)的互连入网，充分利用现有网络资源，发挥主干网的优势。根据未来业务的增长和变化，网络可以平滑地扩充和升级，最大程度的减少对网络架构和现有设备的调整。

3 分层设计

3.1 系统分层结构

系统的分层结构如图 4-1 所示。按照逻辑层次，从下到上分别是基础实施层、系统平台层、应用平台层、应用层。

基础实施层是系统的物质基础，包括互联互通的网络，部署在各地的服务器、存储设备、安全设备和其他各种运行环境设施。这些基础设施将分散部署，从而为系统的数据和业务容灾提供物质基础。集中部署的基础设施在一次灾害中极可能被全部损毁，只有多地分散部署才能提供抗毁的基础设施。



图 4-1 旅游产业云分层结构

系统平台层以数字有机体系统为核心，整合现有的、成熟的、先进的其他系统软件，为应用系统提供强大的系统支撑，使各个应用系统都能按需获得海量的存储空间，高效的数据共享和访问服务、抗毁的数据存储和抗毁的业务运行支持等，并获得高性能、高可靠和高扩展的数据库服务。同时，系统平台层为各种操作系统下的应用提供统一的部署环境，使得这些应用能够共享计算设备、存储设备和数据等。

应用平台层将提供支撑旅游产业应用的基础服务。这些基础服务包括旅游产业数据整合、交换、整理、分析和挖掘等。通过这些服务，旅游产业管理机构可

以发现许多隐藏在大量数据中的规律，比如旅客潜在增长点、旅客消费行为特征、景区旅客流量等。

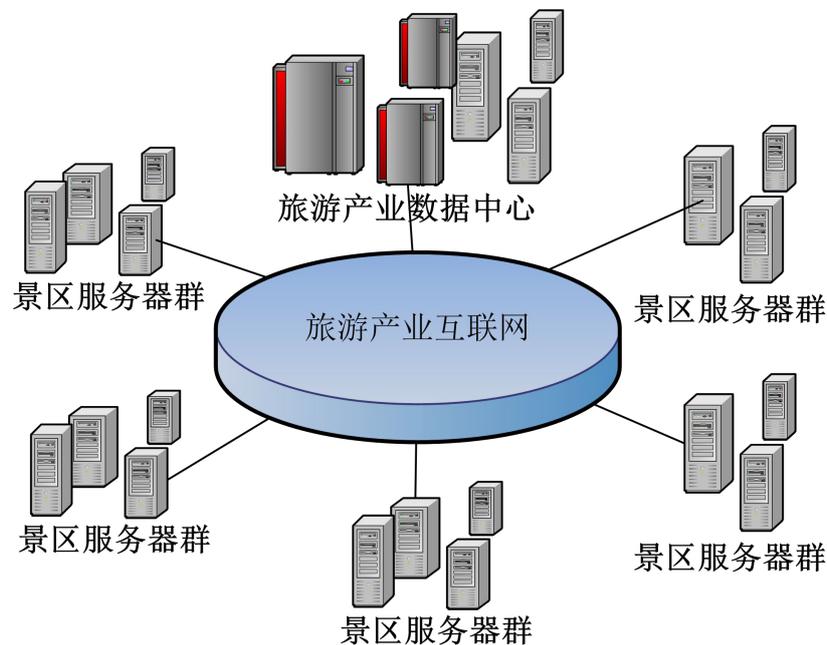
在最上层，将根据需要构建各种应用，如票务系统、通关系统和旅游公共服务门户等。

3.2 基础设施层设计

3.2.1 物理部署结构

旅游产业云的物理部署结构如图 4-2 所示。系统将依托运营商在全省的高速覆盖网络，在各个景区和运营商机房部署服务系统和数据中心，形成即分散又集中的旅游产业云。

在各个旅游景区，就近部署服务器群，为本景区的各种应用业务提供服务。这样，无需很高的骨干网络带宽，景区内的各个应用也能获得很好的网络服务，不会因为骨干网络上的故障而造成景区无法正常运转。各个景区通常都在远离城市的、地质灾害频繁的地方，互联网络难免因为各种原因而中断。因此，必须确保在互联网中断的情况下，景区的信息化系统仍然能够正常运行。



在旅游产业数据中心机房，按需部署各种服务器，为各种旅游产业应用提供后台支持和公共服务。这些后台支持比如旅游产业的大数据分析服务，公共数据存储服务，后台数据处理服务等。同时，可以建立旅游公共服务门户，为各个旅游应用提供共同入口。

从业务逻辑来看，系统可能存在层次关系。各个景区的服务器群主要为本景区提供服务，而旅游产业数据中心则为各个景区的服务系统提供服务。从数据流向来看，各景区的原始数据将收集到旅游产业数据中心，以便进行深入分析和挖掘，然后再向各个景区的应用系统提供高价值的知识。但是，这种层级结构只是体现在业务逻辑层面，并不是物理系统的逻辑结构。

实际上，如果将景区的服务器群也看作一个小的数据中心，则所有数据中心在系统逻辑上是平等的，它们共同组织为一个系统。和其他方案不同，系统中的每个数据中心并不是孤立的，也不是只为本区域的用户提供服务。在这个系统中，所有的数据中心，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。每个数据中心，基于就近服务的原则，将主要为本景区的用户提供服务。但是，在其他数据中心负载过重，或者其他数据中心故障的时候，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与管理系统的整合下，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。本方案也不建议采用昂贵的网络存储系统来构建集中的海量存储系统。这样的存储系统很难满足边远景区的在线存储需求，也无法很好的提供给边远景区的服务系统使用。因此，本方案建议采用廉价的主机内置存储或者磁盘阵列来构建分散部署的存储池。这些存储设备部署在各地，连接到本地的服务器，在数字有机体系统的整合下，形成一个共享的存储系统。边远景区的在线数据就近存储在本地，同时复制到旅游产业数据中心，离线数据才集中存储在旅游产业数据中。在本地存储空间不足时，也可就近存储在其他数据中心。同时，存储系统内的数据，依照访问控制安排和组织关系，可以被全系统的其他用户共享。

考虑到应用逐步部署，业务逐步扩展的需要，可先建立小规模旅游产业数据中心，并整合部分景区的应用系统。然后再根据应用和业务扩展的需求，不断追加部署，整合更多景区的应用系统，最终形成覆盖全省，产生巨大效益的旅游产业云。

这个部署结构结合数字有机体系统将形成具有高抗毁能力的有机系统。它能够分散网络流量，均衡各地业务负载，提升服务效果，增强系统存储和承载能力，满足各种应用的部署需求。

3.2.2 旅游产业数据中心的部署结构

在旅游产业数据中心内，主要设备的部署结构如图 4-3 所示。整个系统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。

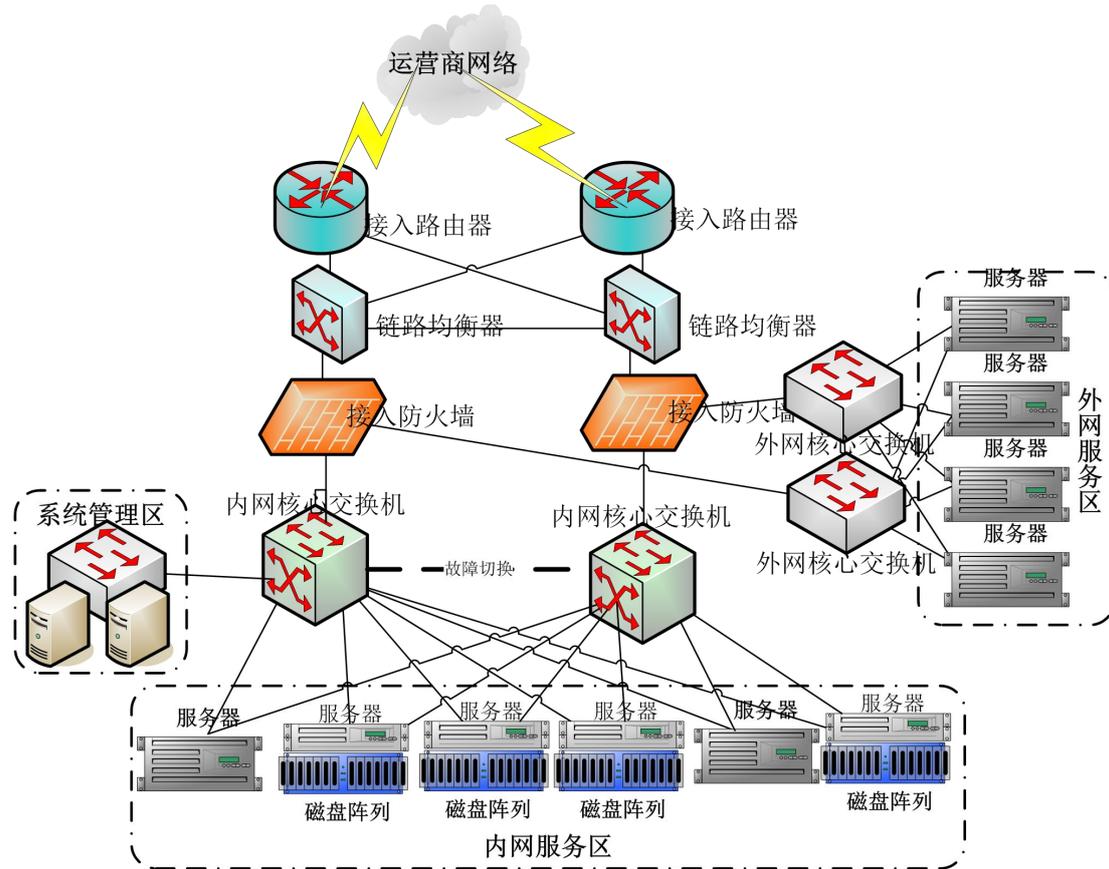


图 4-3 旅游产业数据中心的内部物理结构示意图

3.2.2.1 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：

1) 多链路接入，实现流量均衡和链路备份

这部分主要由接入链路、接入路由器和链路均衡器完成。旅游产业数据中心需要为全省的公众用户和景区系统提供服务，单条链路无法提供充足的带宽扩展，也存在单点故障问题，因此建议采用多链路接入方式，并通过硬件设备实现流量均衡和链路备份。

在本方案下，各个数据中心之间也存在着一一定的网络流量。这个流量不是汇聚型的，而是每个数据中心都需要和其他各个数据中心通信。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。

各个景区的服务系统在与旅游产业数据中心的网络中断的情况下，将独自为本景区提供服务。在网络故障排除后再自动加入系统。

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

考虑到单一设备无法保证长时间百分之百正常运行，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。

3.2.2.2 外网服务区

外网服务区用于部署向互联网公众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连接外部用户。

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。

3.2.2.3 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

根据旅游产业应用发展的规模，内网服务区将部署几台到上千台服务器。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与管理系统的整合下，所有服务器的存储空间将整合在一起，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。单个数据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，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工作库。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工作库服务系统（由分散部署在多地的，数量根据需要决定的服务器构成）。数字有机体工作库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。

5) 大数据处理支撑

数字有机体系统利用部署在内网服务区的服务器实现大数据处理。数字有机体系统将数据分散存储在这些服务器中。这些数据可以存储为文件，也可以数据对象的方式存储，也可以存储在数据库中。数字有机体系统提供基于分布式对象

的远程过程调用机制，使数据分析可以同时大量服务器上并行执行，从而快速的获得结果。该机制支持同时处理大量文件和数据对象，无需整合离散的数据文件，因此使用起来更加方便。该机制采用 C 语言实现和编程，具有更好的处理性能。

数字有机体工作库还提供基于表分片存储的数字有机体查询处理机制。它可以整合多台服务器的处理能力来完成海量数据的查询分析，从而解决海量结构化数据的分析问题。

3.2.3 景区服务系统部署结构

在各个景区，就近部署基础实施，满足本地应用部署和服务的需求。一个景区内物理部署的结构如图 4-4 所示。

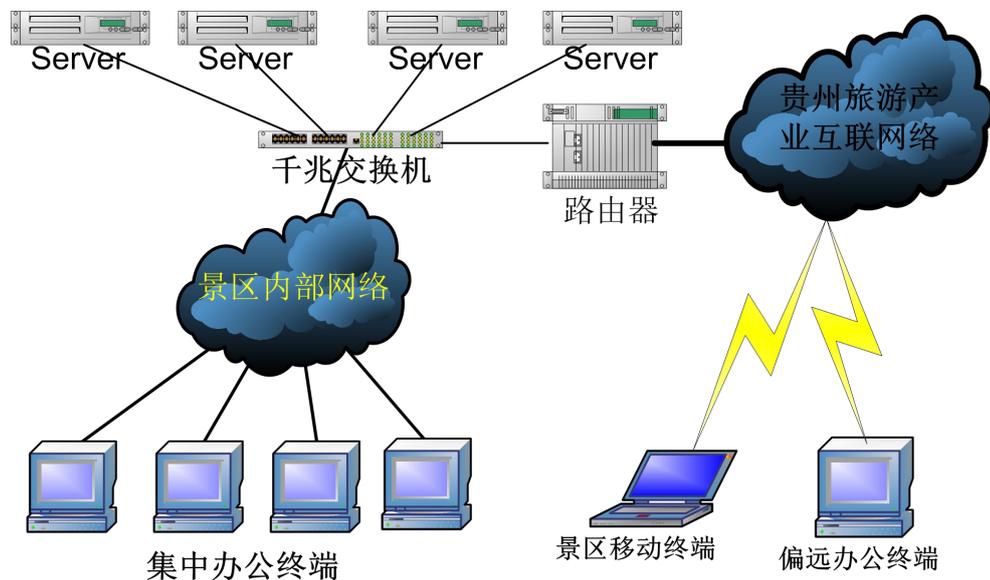


图 4-4 单个景区内部的部署结构图

在一个景区内，需要部署就近提供服务的服务器群。这些服务器可以采用各个景区现有的服务器，从而保护已有投资，减少建设投入。通常各个景区也构建了内部的办公网络，因此也沿用这个网络连接景区内的各种固定终端，从而避免重复网络建设。对景区内的移动终端或者偏远办公点的终端，可以采用移动网络互联，从而解决移动设备和偏远地点难以接入的问题。

建议整合各个景区的互联网门户，统一在旅游产业数据中心提供服务，避免在各个景区单独建设，从而解决重复建设问题，增加系统安全，降低系统投入。这样，各个景区也无需建设独立的互联网服务区，也就无需投入大量的安全设备来保护互联网服务系统的安全。

每个景区可以根据自身的规模增减服务器的数量。本地部署的服务器最少可

以只有一台，最多可达数十甚至上百台。而且，可以随着业务量的增长在线增加服务器，无需重新建设，也无需停机。所有服务器由数字有机体系统整合为一体，用以承载各种应用，并根据应用需求来分配资源。

由于景区内的大量业务都由本地服务器完成，因此和旅游产业数据中心的数据流量主要来自离线数据收集和某些公共服务，需要的带宽相对于集中部署的系统来说要小。而且本地业务开展不依赖旅游产业数据中心，因此即使外联网络中断，本地的大多数业务也不会受到影响。根据各个景区离线数据收集和公共服务的需求，可以动态扩展接入带宽。这样可减少每个景区在网络接入上的投入。

3.3 系统平台层设计

3.3.1 系统平台层结构

系统平台层以数字有机体系统为基础，集合当前成熟的、先进的开源系统软件，构建支撑各种应用的系统平台。数字有机体系统(英文名称为 Digital Organism System，缩写为 DOS)是在刘心松教授带领下，由成都天心悦高科技发展有限公司的研发人员前后千余人次，经过三十多年的技术积累，研发成功的基础系统。

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。研发这种系统的原始宗旨是向生物特别是人类个体和群体的结构、机理和特性逼近，是一种人能化的新的系统模式。这种系统集操作系统、数据库系统、大规模存储、抗毁容灾、高伸缩、高智能、高灵活、自搜索、自传播、自复制、自修复、自重构、自适应、系统间的兼容性、群体间的协作性、对资源的动态管理调度合理配置、大小新旧机器混合使用等特性为一体，是一个整体解决方案，是面向所有应用的统一的（应用）系统平台。

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、中心站或者中心系统，具有良好的自组织性。

系统平台层的内部结构如图 4-5 所示。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、工作库管理系统、大规模存储与管理系统、抗毁容灾系统、虚拟机管理系统、DOSRPC、安全子系统和平台管理系统等。



图 4-5 系统软件层次结构

3.3.2 系统平台层主要功能模块简介

3.3.2.1 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。它主要实现以下几个方面的功能。

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数据中心（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数据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。

3.3.2.2 大规模存储与管理系统

大规模存储与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。存储分配还实现了配额机制。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。

3.3.2.3 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、工作库管理系统等配合，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。

本方案利用数字有机体系统的抗毁容灾功能全面实现旅游产业云中各种应用系统的数据和业务抗毁容灾，从而一举解决系统的可靠性问题，无需为系统灾备单独投资。

3.3.2.4 工作库管理系统

工作库管理系统由数字有机体工作库实现。它是一个支持大规模部署的数据库管理系统。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。

3.3.2.5 虚拟机管理系统

数字有机体系统的虚拟机管理系统满足多数据中心大规模部署和统一管理的需求，虚拟机管理子系统的框架如图 4-6 所示。



图 4-6 数字有机体系统的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。

3.3.2.6 大数据处理支持

数字有机体系统为大数据处理提供了 DOSRPC 编程模型。数字有机体系统具有特有的大数据处理编程模型，即分布式对象的并行远程过程调用机制，简称 DOSRPC。数字有机体系统提供了完善的文件管理系统，因此大量相关数据可以

组织在一个目录树中，从而便于分别访问、处理和分析。这样，海量数据其实是依照自然的逻辑关系组织在大量文件中的，而不是单个文件中。

DOSRPC 以并行远程过程调用的方式实现数据分析处理。编程人员编写处理单个文件或者文件分块内数据的函数，然后指定要执行该函数的文件集合；由系统根据指定的文件集合，以及每个文件或者文件分块的存储位置，自动在数据存储节点上执行数据分析函数，并以函数调用的方式将结果返回给调用者。调用者整合返回结果即可获得数据分析结果。如果数据分析流程很复杂，可以将分析流程划分为多个 DOSRPC 调用。前一个 RPC 调用将分析结果聚合到一些文件中，后一个 RPC 再对这些文件进行分析，从而以并行的方式完成整个数据分析工作。另外，DOSRPC 机制自动实现系统主机间负载均衡，无需编程人员参与任务的分派工作。当系统中某些节点故障时，DOSRPC 机制也自动屏蔽故障，选择其他可用节点执行任务，从而极大地简化编程人员的工作。

例如，要分析一天中不同时间段的旅客流量趋势。为此，可以将一个景区一天的票务流水信息存储在一个文件中，同一个景区的文件先按照月份组织在一个目录下，然后月份目录再按照年份组织，最后上层目录是景区名称。编程人员可以编写一个函数来实现每个文件中一天不同时间段的旅客流量统计，其结果写到一个按日统计文件中。然后再编写一个函数来整合一个月的数据，以此类推，编写整合每年、每个景区、全省的数据的函数。当需要分析某个景区某月的情况时，只需以该景区该月的目录为参数调用第一个 DPRPC 函数，然后再按照生成文件规则指定第二个 RPC 函数的文件集合即可获得数据。如果要分析全省所有景区某年的情况，则以最上层目录为参数调用第一个 RPC 函数，然后按照文件生成规则依次调用其他 RPC 函数即可获得结果。这样，在分析某个景区某个月的数据时，就无需检索其他月份，或者其他景区的数据，大大的提高了处理效率。

3.3.2.7 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机制。这些安全机制为建设高安全的云平台提供了全面的支撑。

3.3.3 统一业务运行

建立旅游产业云的一个根本目的是实现所有业务的统一运行和管理，即建立统一的业务运行平台。而判断是否建立起统一的业务运行平台则需要从能否实现

资源共享、协同服务和统一管理，以及实现到什么程度来衡量。

考虑到在旅游产业云中运行的业务系统很多，而且这些业务系统采用不同的操作系统，需要不同的硬件环境。因此，单一的业务运行方式无法满足各种业务的运行需求。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。

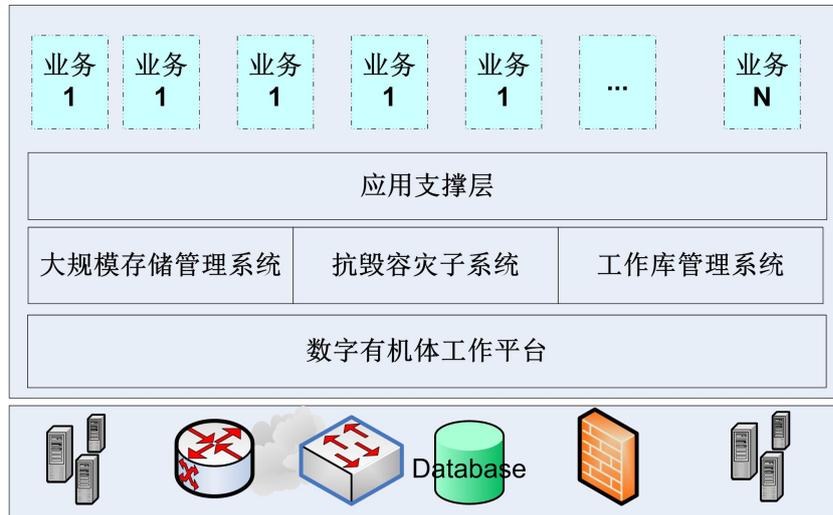


图 4-7 数字有机体系统的“沙箱”运行模式

采用“沙箱”运行方式的逻辑结构如图 4-7 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。

数字有机体系统也提供虚拟机运行方式，其概念结构如图 4-8 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。

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。



图 4-8 虚拟机运行模式的逻辑结构

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 操作系统的 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。

无论是那种方式，数字有机体系统都很好地实现了资源共享、协同服务和统一管理。各个业务可以运行在各台服务器上，共享所有服务器的计算资源、存储资源和网络资源等。在数字有机体系统的组织下，他们协同对外提供服务，实现负载均衡、流量均衡、抗毁容灾等，具有良好的协作能力。同时，由统一的运维管理系统管理，实现统一管理的目的。

3.3.4 高可靠、高扩展的共享存储系统

数字有机体系统可以为各种业务系统提供可靠的共享存储系统。对以“沙箱”方式运行在数字有机体系统内的业务，可以通过文件系统服务和数据库系统服务的方式提供共享存储服务。系统管理员为业务建立一个账号，并分配相应的配额，然后为业务建立一个自有的文件系统（类似于分区）即可。业务系统使用这个账号可以在任意服务器上访问这个自有文件系统，并在配额限制范围内使用存储空间。业务系统无需关心具体的存储设备在哪里，也无需关心文件具体存储在哪里。它完全就像在访问一个本地的存储系统一样。系统管理员可以动态地调整业务系统的存储配额，从而满足业务系统的存储需求变化。各个业务系统共享同一个虚拟存储池，减少存储资源闲置。各个业务系统的自有文件系统互不关联，从而实现了业务间的隔离。

对以虚拟机方式运行的业务，数字有机体系统将虚拟存储池中的空间以虚拟磁盘的方式提供给虚拟机使用。虚拟机的虚拟磁盘实际上是数字有机体文件系统中的多个文件，从而实现各个业务共享存储系统。

这个存储系统是高可靠的，它自动复制系统中的文件和数据记录，包括异地复制，从而使得存储服务不会因为某个存储磁盘、或者某个存储设备的损坏而停止。业务系统可以获得连续不断的存储服务，从而为业务的抗毁容灾提供坚实的支撑。这是许多共享存储解决方案无法实现的。

这个共享存储系统也是高可扩展的。它不会受限于任何单一设备。你可以扩展每台服务器的存储容量，也可以为系统增加服务器，甚至增建更多的数据中心，从而无限制的扩展这个共享存储池的容量。这也是其他共享存储解决方案无法实现的。

3.3.5 全面抗毁容灾

在本方案中，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，当某些数据中心故障时，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。

3.3.5.1 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。根据旅游产业云的部署结构和业务逻辑，建议采用如下的复制策略：

各景区存储本地的在线服务数据，并同步复制到旅游产业数据中心；离线数据则异步复制到旅游产业数据中心，形成离线数据汇集。

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。

对重要数据建立离线备份机制，各地将自己的重要数据离线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。因此本方案已经提供了足够的数据高可用性保障。

3.3.5.2 业务抗毁容灾

数字有机体系统为业务抗毁提供了以下支持：

1) 通过数字有机体文件系统，运行在各个数据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，运行在各个数据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数据中心被摧毁后，业务迁移到其他数据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) 各个数据中心间互联互通，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数据中心，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（含数据中心内负载均衡，多数据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，本方案建议采取如下的业务容灾策略：

由于各个数据中心都可作为其他数据中心的冗余备份，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。

无需单独建设备份中心，也无需单独建设数据容灾系统。

配置各个数据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，直接采用多数据中心并行服务的方式（各数据中心内部又可采用多机并行服务方式）。对只需为本数据中心用户提供服务的业务，采取本数据中心多机并行服务方式，并配置多个备份异地数据中心，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数据中心，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。

3.4 系统安全

3.4.1 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。系统可靠性内容前面已经描述。本方案的安全框架如图 4-11 所示。其中，物理安全、网络安全、应用安全、安全制度、安全管理、漏洞评估与扫描、信息安全标准规范和条例、实施方案等在许多解决方案中都能找到，因此本方案就不再累述。



图 4-11 安全体系示意图

本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。

3.4.2 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于 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，它完全可以为旅游产业应用提供坚实的

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。

3.4.3 数字有机体工作库的安全

数字有机体工作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。

4) 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，从而使得数字有机体的数据库安全特性进一步增强。

3.4.4 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。

3.5 统一运维

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 4-12 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。

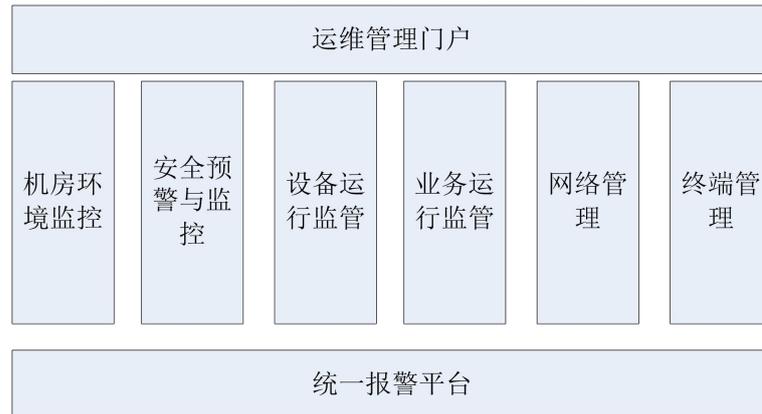


图 4-12 运维管理信息系统结构

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) 电子地图上各数据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；

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，建立数据中心间的层级关系。每级数据中心的管理人员可以管理自身数据中心以及下面各级数据中心的各个子系统。因此，可以由上级数据中心代管下级数据中心，下级数据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景区服务系统的人力开销。

4 系统的优点和特点

本方案具有以下优点和特点。

1) 高扩展性

系统可以从小规模旅游产业数据中心起步，整合少数旅游景区的业务系统，

再逐步建设更大规模的数据中心，移入更多的业务，整合更多旅游景区的业务系统，从而随着业务的不断发展而扩展，最终满足全省所有景区各种各样的应用需求。逐步扩展系统使得无需一次完成大量投入，并且可以通过滚动发展方式，实现边投入边获益，以确保可持续地发展。

2) 高可靠性

系统在文件系统和数据库内实现人能化地复制，数据可以同时复制到多个异地系统中，同时支持异步同步和实时同步，满足各种业务对数据同步的需求和可靠性需求。同时在数字有机体系统的支持下，业务可以做到不间断服务，满足系统对高可用性的要求。高可靠性消除了系统因为各种原因而停机的风险，使得重要业务能够放心的部署到平台中。

3) 高安全

整个系统由国产化的软件建立核心平台，不担心存成“后门”。数字有机体系统从操作系统内核和数据库核心实现各种增强的安全机制，确保基础平台安全。构建可靠的完整的应用安全支撑，为各种应用提供安全服务，确保各种应用能够安全可靠的运行。高安全性确保各种应用系统能够放心的在数据中心中运行，而无需担心机密信息泄露。

4) 良好的业务承载能力

系统针对不同的应用需求提供两种业务承载方式。对可以在 Linux 下运行的，需要大规模分布式部署的业务，如教育资源共享等，提供“沙箱”运行方式，使得业务系统能够具有无限扩展的服务能力。对已有的 Windows 业务采用虚拟机运行方式，使其可以快速部署在数字有机体系统上。

5) 丰富的应用支撑

从头开始在一个新的平台上开发旅游产业云中的各种业务不仅费时费力，而且可能面临巨大的技术风险。数字有机体系统为旅游产业云中的典型业务，如票务系统、通关系统、门户系统等提供了完善的现成应用平台，可以根据用户需求快速的开发出满足需求的业务，避免“云”建设常见病：“有路无车”。

6) 是实现旅游产业云的理想“云”解决方案

传统的基础实施即服务方案适用于整合小业务，以提升大服务器的利用率，却不适用于需要满足大量分散异地网络用户的在线业务。因为它无法整合大量分散部署的服务器。而应用即服务的云方案显然也存在同样的问题，在景区外联网络故障时，这种方案将使整个景区瘫痪。在平台即服务的方案中，常见的以 Hadoop 为基础的云计算方案只适用于处理大数据，并不适用于提供在线业务服务，例如票务系统。而基于数字有机体系统的云方案支持大规模分散部署，支持就近提供服务，支持在线业务，提供各种高可用、高扩展、大数据处理等支撑，是最理想的解决方案。

7) 无限伸缩的海量存储

本方案支持海量数据存储。每台服务器可以内置高达 16 块的磁盘，也可外接磁盘阵列甚至 SAN 等存储系统。每个数据中心可以部署多达数十台服务器，整个系统可以根据需要建立更多的数据中心，从而满足系统存储容量和处理能力的不断扩展。

8) 就近服务和负载均衡

系统在调度任务时，采取就近服务优先，兼顾负载均衡的原则。用户总是访问离自己最近的数据中心。在就近的数据中心能力不足时再调度到其他数据中心。这使得各地的用户都像在访问本地数据中心一样，不存在网络距离远，访问不畅通等问题。系统兼顾负载均衡，使整个系统具有良好的访问性能。

9) 高性价比

系统无需采用负载均衡器和小型机等硬件设备，也无需购买昂贵的 Oracle 数据库、EMC 的存储设备等。整个系统采用高性价比的通用服务器和磁盘阵列等构成。系统的总体投资低于采用传统技术的方案。

10) 统一运维管理

为整个系统建立统一的运维管理平台，使系统维护人员可以在上级数据中心统一维护和管理分散在各地的数据平台和业务系统，从而保证系统的维护方便性，减少维护费用。

5 客户价值

1) 全面抗毁容灾，运行安全无忧。系统从物理部署、数据和业务三个层面屏蔽各种故障，自动应对各种问题，尽力使业务系统保持运行。

2) 具有大数据处理能力，使实时大数据分析成为发掘旅游商机的利器。系统全面支持大数据的存储、处理、分析和应用，为结构化和非结构化大数据提供直接的全面的处理能力，从而应用人员可以快速开发出灵活的实时大数据分析工具，及时发掘各种旅游商机。

3) 为整合应用提供全面的支持，使资源得到充分利用。解决方案既提供平台即服务、应用即服务的云计算能力，也提供基础实施即服务的云计算能力。可以从共享基础实施、共享业务平台和共享应用三个层面整合各种应用系统。

4) 安全可靠。数字有机体系统从操作系统、数据库开始增强信息系统的安全性，而不仅靠网络安全设备或者某个公司的安全产品来保障系统的安全。

5) 统一运维，管理方便。解决方案提供多层面的，完善的运维系统，使分散部署的系统也能集中维护和管理，降低系统运行费用。