第五章　本期项目设计方案

6、数据处理和存储系统设计

针对用户的业务状况和发展趋势，我们建议用户采用以数据和存储为中心的系统结构。以数据和存储为中心可以极大地保护用户的投资，有效利用存储空间，降低用户管理费用，从而确保整体拥有成本最低。降低管理难度，维护数据管理的统一性。提高了电子化数据管理的可靠性。数据的集中化管理，能够确保数据的一致性和完整性，保证电子化数据的可靠性。

以数据和存储为中心必然对整个存储系统I/O有很高的要求，所以我们建议用户选用集中式，高性能，大容量，智能化的存储区域网(Storage Area Network，简称SAN)来构建新一代计算中心存储环境。

采用以数据和存储为中心的SAN解决方案，集中的解决了系统体系结构中对存储I/O性能和数据库应用共享的挑战，它的主要特点为：

**l)开放的标准，适合于服务器和存储设备之间的共享**

SAN标准最早就是为了多个服务器之间通过专用的高速网络来共享存储和更加有效地管理存储设备所设计，经过近十年的发展，已经成为非常完善的标准。各主流厂商均遵循开放的观念，保证各家设备之间的互连性。在物理连接上是采用已经成熟的光纤技术实现。由于ERP系统规模比较大、各项应用和各种设备都比较多，SAN的这一点优势尤为重要，在系统改造、升级中将能够很好的利旧。凭借惠普在服务器和存储方面丰富的经验和技术，惠普的SAN方案使用户能迅速、方便地建立、整合和管理其多平台的存储环境，让用户对其异构存储局域网拥有无限的扩展能力、管理能力和百分之一百的可用性。

**2)高性能的数据存取**

SAN采用的链路连接是通过光纤，光纤本身具有抗干扰能力强，传输距离长，传输速度快的特点，目前具有的速度是4Gbit/s。而且最关键的是，基于SAN架构，服务器和存储设备之间的协议是专为数据密集型存取所设计。

**3)具有高度的可扩充性**

基于SAN架构的存储设备，本身具有可扩充性。而且一旦SAN架构构建以后，可以很容易增加存储设备，并且这些存储设备均可以作为一个整体来共享，它们可以作为一个卷或多个卷来共享。在SAN的架构下，存储是独立于应用的。

**4)具有无与伦比的可靠性**

作为关键性应用中，设备的可靠性是必须考虑的。在SAN架构中，主机和光纤交换机，和存储设备之间的连接均是冗余的，冗余的通路带来的好处，在正常情况下，是带宽的扩充，实现自动负载均衡，如果某一通路出现问题，它又可以作为另一选择路径，保证系统的可用性。

SAN的存储设备内部，本身也考虑很多系统的高可用性，如惠普磁盘通常是连接到两台光纤环路上或两个控制器上，内部的总线或连接也均是多通道的，电源，风扇等等均是冗余的。

**5)基于SAN的备份恢复、灾难恢复等多种解决方案**

目前具有多种基于SAN架构的解决方案，比较典型的是包括远程容灾解决方案和零停机时间备份。它可以通过异地远程的两台阵列实现数据的同步，独立于操作系统和应用，一旦某地的系统出现问题，可以很快地切换到异地，保证系统的应用。数据的备份和恢复也是一个数据密集型访问的应用，如果基于LAN，要占用企业内部大量的带宽，前台响应将极为缓慢，因此，在SAN的架构下，可以实现LAN-free的备份解决方案，Severless的备份解决方案和零停机时间的备份解决方案。

**6)集中式管理**

分布式的设备，包括主机系统、存储系统、交换机和光纤适配器等等，均可以通过一个简单的管理平台从单点管理，可采用HP OpenView Storage Area Management软件平台。

1. 终端系统及接口设计

**1.云桌面概述**

**1.1 云桌面简介**

　　在计算机中的桌面是指打开个人计算机并登录到操作系统后看到的主屏幕区域，这就是我们工作的桌面。云桌面也是一个显示在我们屏幕上的桌面，但它的后面不是一个真实的计算机，而是通过网络连接远端服务器上。也就是说，云桌面是由服务器提供的，所有的数据计算运行在服务器上，云桌面仅仅显示桌面图像，并接受键盘、鼠标等[外设](http://articles.e-works.net.cn/IO/" \o "外设" \t "http://articles.e-works.net.cn/infrastructure/_blank)的输入操作。服务器能同时为多人提供不同桌面，如Windows桌面、Linux桌面等。我们只需要一个客户端设备，或者其他任何可以连接网络的移动设备，通过浏览器或者专用程序，就可以访问驻留在服务器的个人桌面。用户体验和我们使用传统的个人电脑是基本一样的。

　云桌面的接入终端一般是瘦终端或者普通PC(个人计算机)。部分云桌面系统也支持智能手机、Pad等终端接入设备。接入终端用以处理与服务器间的远程连接协议、输入输出设备、外围设备驱动等，并将终端连接设备映射到服务器会话中，用户可以执行保存、打印、输出操作。

**1.2 云桌面架构**

　一个云桌面系统的典型架构可分为终端接入、云桌面系统和访问的业务系统3个层次，见图1。

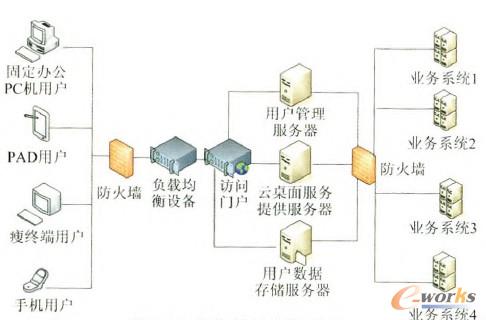
[ 放大图片](http://articles.e-works.net.cn/articles/articleimage/20143/130389988663235209_new.jpg)

图1 云桌面系统典型架构

　云桌面工作流程：用户通过各种终端通过桌面显示协议访问云桌面接入地址或门户，该访问地址或接入门户一般前置负载均衡设备。由用户管理服务器，通过用户管理系统，通常是微软的AD(活动目录)验证用户身份，认证通过后请求被定向到随机或定制的云桌面。用户登录云桌面后，如同登录本地桌面一样访问业务系统进行操作。

**2.云桌面的两种主流技术**

**2.1 两种主流技术介绍**

根据云桌面不同的实现机制，目前主流云桌面技术可分为两类：虚拟桌面基础架构的VDI(虚拟桌面基础设施)方式和基于服务器计算模式的SBC(基于服务器计算)方式。

　VDI方式：在数据中心通过虚拟化技术为用户准备好安装Windows或其他操作系统和应用程序的虚拟机。用户从客户端设备使用桌面显示协议与远程虚拟机进行连接，每个用户独享一个远程虚机。这种技术也可称为桌面虚拟化。

　SBC方式：用户通过与服务器建立不同的连接session(对话)对服务器上的应用进行访问。通过不同的会话区分和隔离用户，使多个用户同时共享同一个操作系统。可通过策略配置为每个用户提供不同的桌面。

　简而言之，VDI是连接到一个独享的虚拟机，而SBC是连接到共享的终端服务器的session。

**2.2 两种技术对比**

　相对于SBC方式，VDI的优势在于：

　1)多操作系统支持。SBC方式下用户只能接入Windows系统。VDI方式下，用户可以接人Windows或Linux操作系统。

　2)更好的性能和安全性。SBC是多用户的session共享同一个操作系统，而VDI是每个用户都有自己独立的虚拟机，用户可拥有独立、完全的桌面使用和控制权限。如果其中一个用户虚拟机出错，不会影响到其他用户。在计算性能、数据的安全性和隔离性上，VDI方式优于SBC方式。

　3)应用软件兼容性支持好。在实际工作中，并不是所有的应用都与终端服务相兼容。由于VDI是独享的虚拟机操作系统，对应用的兼容性更好。

　4)对外设的支持度高。VDI使用的是一个完整的虚拟机，对各类端口的外设支持度高，包括串口、并口、USB(通用串行总线)口，还可将终端连接的不同外设通过桌面显示协议传输数据到服务器端进行二次开发。而SBC是Windows操作系统下共享的会话，部分解决方案不支持USB外设，也无法通过桌面显示协议针对外设传输数据进行二次开发，对外设的支持度较低。相对于VDI方式，SBC的优势在于：

　1)部署成本低。VDI实现的基础是在服务器侧部署虚拟化软件，为用户提供独享虚拟机。虚拟化软件购置需要成本，对计算和[存储](http://articles.e-works.net.cn/Storage/" \o "存储" \t "http://articles.e-works.net.cn/infrastructure/_blank)资源要求也高。相比而言，SBC的实现在服务器侧只需要安装一套操作系统，软硬件成本都较低。

　2)集中管理性好。个性化设置是云桌面用户的实际需求。在VDI方案下，每个用户在虚拟机设置、用户应用设置、用户权限上有不同需求，配置管理文件比较复杂。SBC方式只针对用户访问应用进行控制，降低管理难度。

　3)整合比更高。将一台服务器的硬件资源切分给用户session所占用的资源小于切分给用户虚拟机所占用的资源，所以SBC比VDI具有更高的整合比，同一台服务器可服务于更多的用户。

**3.云桌面优势**

　与传统桌面工作方式比较，云桌面具有明显优势。

　1)工作桌面集中维护和部署，提高桌面服务能力和工作效率。云桌面改变了过去分散、独立的桌面系统环境。通过集中部署，IT人员在服务器侧完成所有的桌面管理维护]二作，包括操作系统安装、软件更新、操作系统补丁升级、安装防病毒软件等等。最终使用用户不需要对个人工作桌面自行维护，连接云桌面后可运行的程序“所见即所得”，减少了企业大量的桌面维护工作，也提高了企业桌面维护支持的服务水平。

　2)数据远程隔离，有效保护数据的[信息安全](http://articles.e-works.net.cn/Security/" \o "信息安全" \t "http://articles.e-works.net.cn/infrastructure/_blank)。云桌面的用户桌面环境、业务数据都是托管在远程服务器上，本地终端只是一个显示设备。终端不处理和存储业务数据，通过云桌面系统的策略控制，业务数据无法下载到本地，有效保障了数据的安全。维护人员甚至通过设置不同的本地终端控制策略，禁止用户对本地USB等设备的访问，通过这样的数据隔离措施，企业能够有效的保证数据不被违规带出企业，可有效防范数据的非法窃取和传播。

　3)多终端多操作系统的接人能力。云桌面是由服务器提供的，用户可随时随地通过移动或固定网络访问。部分云桌面平台还支持多种终端的接入，如瘦客户端、PC机、上网本、手机、平板电脑等，支持苹果iOS(操作系统)、安卓等多种系统平台。

**4.云桌面建设方案设计要素**

　云桌面方案只有具备替代现有终端的条件下才有实施意义。在规划云桌面的建设方案时，必须对现有环境进行充分的调研和详细的方案设计，应从云桌面最终用户应用场景、使用的终端外设、对网络的带宽要求、用户云桌面配置要求、投资成本等方面综合考虑。

**4.1 应用场景**

　云桌面方案的关键技术是桌面显示协议，受目前桌面显示协议技术成熟性的限制，对大数据量的传输支持效果较差。如果最终用户是高质量多[媒体](http://news.e-works.net.cn/category638/media.htm" \o "媒体" \t "http://articles.e-works.net.cn/infrastructure/_blank)需求或复杂图形计算的使用需求，则不适合应用云桌面技术来建设。

　此外，远程桌面显示离不开网络传输，每种不同的桌面显示协议对带宽有不同要求。对于网络质量不能保障的应用场景，也不适合应用云桌面技术来建设。采用基于VDI的解决方案，用户能够获得一个完整的桌面操作系统环境，虚拟机之间的数据安全隔离度较好，一个用户虚拟机的宕机不会影响其他用户，这与本地计算机的使用体验十分接近，从而使服务质量得到保障。因此，基于VDI的云桌面比较适合于对桌面功能需求完善的用户使用。采用基于SBC的解决方案，整个方案实施部署对服务器软硬件复合利用度高，但在性能隔离和安全隔离方面较差，共享操作系统方式可能发生软件兼容性冲突，最终用户可访问的是受策略控制的服务器版本操作系统，与本地计算机的使用体验有差距，较适合于应用场景单一、外设标准化程度高的用户。

**4.2 终端外设**

　不同用户的最终应用场景差异很大。对于固定办公使用，一般只需要支持鼠标、键盘、打印机几个标准外设；用于业务受理的营业厅使用则除上述外设外，可能还需要支持扫描仪、身份证识别仪、指纹仪、U-key(USB key)、评价器、POS(销售点终端)磁卡刷卡器等多种复杂外设。云桌面客户端主要是使用瘦终端。在瘦终端选型时，应确保接口型号、数量能够满足运行需要。对应用场景中有特殊驱动、接口或配置的外设，必须提前进行设备驱动识别验证，确保实施要求。

　不同云桌面建设方案采用的桌面显示协议是不同的，终端选型时也要求该终端支持所使用的桌面显示协议。

1. 网络系统设计

根据目前计算机网络现状和需求分析以及未来的发展趋势，在网络设计时应遵循以下几个原则。

**1．开放性和标准化原则**

首先采用国家标准和国际标准，其次采用广为流行的、实用的工业标准，只有这样，网络系统内部才能方便地从外部网络快速获取信息。同时还要求在授权后网络内部的部分信息可以对外开放，保证网络系统适度的开放性。

这是非常重要，而且非常必要的，同时又是许多网络工程设计人员经常忽视的。我们在进行网络系统设计时，在有标准可执行的情况下，一定要严格按照相应的标准进行设计，而不要我行我素，特别是在像网线制作、结构化布线和网络设备协议支持等方面。采用开放的标准后就可以充分保障网络系统设计的延续性，即使将来当前设计人员不在公司，后来人员也可以通过标准轻松地了解整个网络系统的设计标准。保证互连简单易行。

**2．实用性与先进性兼顾原则**

在网络系统设计时首先应该以注重实用为原则，紧密结合具体应用的实际需求。在选择具体的网络技术时一定要同时考虑当前及未来一段时间内主流应用的技术，不要一味地追求新技术和新产品，一方面新的技术和产品还有一个成熟的过程，立即选用时则可能会出现各种意想不到的问题；另一方面，最新技术的产品价格肯定非常昂贵，会造成不必要的资金浪费。

如在以太局域网技术中，目前千兆位以下的以太网技术都已非常成熟，产品价格也已降到了合理的水平，但万兆位以太网技术还没有得到普及应用，相应的产品价格仍相当昂贵，所以如果没有十分的必要，则不要选择万兆位以太网技术的产品。

另外在选择技术时，一定要选择主流应用的技术，如像同轴电缆的令牌环以太网和FDDI 光纤以太网目前已很少使用，因此不要使用了。目前的以太网技术基本上都是基于双绞线和光纤的，其传输速率最低都应达到10／100Mbps。

**3．无瓶颈原则**

这一点非常重要，否则会造成花了高的成本购买了主档次设备却得不到相应的高性能。网络性能与网络安全一样，最终取决于网络通信链路中性能最低的那部分。

如某会聚层交换机连接到了核心交换机的1 000Mbps双绞线以太网端口上，而该会聚层交换机却只有1 00Mbps，甚至1 0Mbps的端口，很显然这个会聚层交换机上所连接的节点都只能享有】0Mbps，或者1 00Mbps的性能。如果上联端口具有1 000Mbps性能，而各节点端口支持1 00Mbps连接，则性能就完全不一样了。

还如服务器的各项硬件配置都非常高档(达到了企业级标准)，但所用的网卡却只是普通的PCI l O／1 00Mbps网卡，显然这又将成为服务器性能发挥的瓶颈。再好的其他配置，最终也无法正常发挥。再如，服务器的处理器达到了4个至强处理器，而内存容量却只有初始配置的1 GB，或者磁盘采用了读写性能较低的IDE RAID，或者SATA RAID，这样配置的结果同样会使服务器的性能大打折扣，浪费了高性能配置资源。

这类现象还非常多，在此就不一一列举了。这就要求在进行网络系统设计时一定要全局综合考虑各部分的性能，而不能只注重局部的性能配置。特别是交换机端口、网卡和服务器组件配置等方面。

**4．可用性原则**

我们知道服务器的“四性”中有一个“可用性"，网络系统也一样。它决定了所设计的网络系统是否能满足用户应用和稳定运行的需求。网络的“可用性"其实就是表现在网络的“可靠性…‘稳定性"，要求网络系统能长时间稳定运行，而不要经常出现这样或那样的问题。否则给用户带来的损失可能是非常巨大的，特别是大型、外贸、电子商务类型的企业。当然这里所说的“可用性"还表现在所选择产品要能真正用得上，如所选择的服务器产品只支持UNIX 系统，而用户系统中根本不打算用UNIX系统，则所选择的服务器就用不上。

网络系统的“可用性’’通常是由网络设备(软件系统其实也有“可用性”要求)的“可用性"决定的，主要体现在服务器、交换机、路由器、防火墙等重负荷设备上。这就要求在选购这些设备时一定不要一味地贪图廉价，而要选择一些国内、外主流品牌、应用主流技术和成熟型号产品。对于这些关键设备千万不要选择那些杂牌，一方面性能和稳定性无法保障，另一方面售后服务更将是无法弥补的长久的痛。

另外，网络系统的电源供应在可用性保障方面也非常重要，特别是对于关键网络设备和关键用户机。这时就需要为这些节点配置足够功率的不问断电源(UPS)，在试电出现不稳定，或者停电时可以持续一段时间供用户保存数据、退出系统，以免数据丢失。通常像服务器、交换机、路由器、防火墙之类关键设备要接在有1个小时以上(通常是3小时)的UPS电源上，而关键用户机则需要接在支持1 5分钟以上的UPS上。

**5．安全第一原则**

网络安全涉及到许多方面，最明显、最重要的就是对外界入侵、攻击的检测与防护。现在的网络几乎时刻受到外界的安全威胁，稍有不慎就会被那些病毒、黑客入侵，致使整个网络陷入瘫痪。在一个安全措施完善的计算机网络中，不仅要部署病毒防护系统、防火墙隔离系统，还可能要部署入侵检测、木马查杀系统和物理隔离系统等。当然所选用系统的具体等级要根据相应网络规模大小和安全需求而定，并不一定要求每个网络系统都全面部署这些防护系统。

除了病毒、黑客入侵外，网络系统的安全性需求还体现在用户对数据的访问权限上，一定要根据对应的工作需求为不同用户、不同数据配置相应的访问权限，对安全级别需求较高的数据则要采取相应的加密措施。同时，用户账户，特别是高权限账户的安全也应受到高度重视，要采取相应的账户防护策略(如密码复杂性策略和账户锁定策略等)，保护好用户账户，以防被非法用户盗取。

在安全性防护方面，还有一个重要方面，就是数据备份和容灾。这非常重要，在一定程度上决定了企业的生存与发展，特别是企业数据主要是电子文档的电子商务类企业。在设计网络系统时，一定要充分考虑到用户对数据备份和容灾，部署相应级别的备份和容灾方案。如中小型企业通常是采用Microsoft公司Windows 2000 Server、Windows Server 2003系统中的备份工具进行数据备份和恢复，而对于大型的企业，则可能要采用第三方专门的数据备份系统，如Veritas(维他斯，现已并入赛门铁克公司)的Backup Exec系统。

9、安全系统设计

### 应用层安全设计

CA已经实现政务数字证书的受理与发放，并建立基于数字证书技术的应用安全支撑平台，包括面向内部用户的统一认证管理系统、面向社会公众的认证服务系统、提供数据安全传输的密码服务系统和确保电子文件责任性的电子签章系统等部分，基础地理数据及数据服务平台各个应用系统将利用CA提供的可信认证、完整性保护、权限验证、责任认定等基本安全服务功能，实现各类应用系统的安全互联互通、安全信息共享、安全应用整合。

根据需要，基于CA集成来实现用户身份认证和系统安全，建立统一的身份认证系统，严格控制身份鉴别与授权和访问控制，在安全上采用多层面安全保障，以确保业务流程满足安全要求。

应用系统的安全必须以网络安全和系统安全为基础。在安全设计中应着重考虑以下几个方面：

认证与授权服务：应具有单独的登录控制模块对登录用户进行身份标识和鉴别，同时支持多种身份认证方式，如CA证书方式，用户名密码方式和多因子认证等其它认证方式。

程序资源访问控制安全：根据用户的身份和对系统的使用情况将用户分成不同的用户组；为不同的用户或用户组分配不同的系统资源（如对象、数据等）访问权限；用户只能访问到自己有权限访问的系统资源（如对象、数据等）。

功能性安全：明确各个功能的流程上的安全措施，如是否需要审核，文件上传最大限制等。

数据域安全：包括两个层次，其一是行级数据域安全，即用户可以访问哪些业务记录，一般以用户所在单位为条件进行过滤；其二是字段级数据域安全，即用户可以访问业务记录的哪些字段。

应用日志与审计：为关键的系统流程设计日志审计功能。日志中需记录用户对系统敏感资源（如保密数据或文件等）的访问情况；对过期的日志要进行备份，以便日后查阅。

#### 应用开发安全

应用开发安全主要从以下几个方面考虑：

**1、安全编程**

本项目中的所有应用系统都应正确选择程序设计语言和其它程序设计工具，从而提高最终产品的可靠性和正确性；为提高整个系统的安全性，要恰当地选择并利用这些工具帮助防止程序错误进入源编码。

严格采用软件工程的方法编制程序，对编码至少由一名未参与程序设计的程序员检查程序编码，全面了解其安全要点，他与原设计者对程序遗留问题负有同样的责任。

**2、接口安全**

应用系统接口是易受攻击的脆弱点，应从职责管理上加强，将责任实现最佳分离。基础地理数据及数据服务平台项目中涉及到的各类接口，都应尽量标准化，基于总局统一的接口标准规范定义接口，从而利于应用系统间信息的互通。

**3、数据传输的保密性**

对敏感数据以及与基础地理数据及数据服务平台交换的数据应采用加密传输技术以保证数据传输的保密性；必要时采用二次认证方式，实现对数据的保护。

**4、安全审计**

基础地理数据及数据服务平台项目的开发安全应考虑系统对安全审计的支持，审计模块至少包括以下内容：事件的日期、时间、发起者信息、类型、描述和结果等内容，审计记录的内容应当尽可能保证详细，以便事后问题的追踪和审计检查。

**5、安全测试**

在基础地理数据及数据服务平台项目核心征管系统软件与集成平台项目中，综合运用静态和动态检测技术，对软件的安全性进行全面认真的检测和评估，发现在系统设计和编码中的错误、疏忽和其它缺陷。

**6、系统开发安全管理**

建立管理体制包括建立防范组织、健全规章制度和明确职责任务三部分。管理体制是进行管理的基础，规章制度应在权限的分配过程中建立，并可根据需要参照执行。基础地理数据及数据服务平台项目应建立良好的管理体制并归档。

**7、支持外部安全控制措施的整合**

支持基于数字证书的身份认证、权限管理、传输加密、安全中间件的调转等外部控制机制的加入。

#### 身份认证

基于PKI基础设施提供应用系统的身份认证功能。通过安全基础设施，实现数字证书管理、权限管理、密钥管理、密码服务、证书查询与发布、可信时间戳服务等功能，在基础地理数据及数据服务平台项目中，形成统一的信任域和访问控制策略域，实现全系统统一的基于密码技术的身份认证和统一的细粒度访问控制，为全网提供身份认证、安全审计与责任认定、可信时间戳、加密密钥对生成、访问控制、数据保密、数据完整性保护、数据真实性保护、通信抗抵赖性保护等安全服务，提高系统整体的安全性以及安全系统的可控性与可管理性。

#### 访问控制

用户认证可以将非法用户拒绝于系统之外，但对计算机系统来说，不能因为允许一个用户进入系统后，就让他不受任何限制地访问系统中的所有程序、文件、信息等对象。从安全的角度出发，需要对已进入系统的用户的各种访问操作进行控制。同样，对进入网络中的用户也需要进行访问控制，主要体现在以下方面：

**1、防范非法用户的访问**

非法用户的访问也就是黑客或间谍的攻击行为。在没有任何防范措施的情况下，网络的安全主要是靠主机系统自身的安全，如用户名及口令字这些简单的控制。但对于用户名及口令的保护方式，对出于攻击目的人而言，他们可以通过对网络上信息的监听，得到用户名及口令，或者通过猜测获得用户及口令。因此，要采取一定的访问控制手段，防范来自非法用户的攻击，严格控制只有合法用户才能访问合法资源。

**2、防范合法用户的非授权访问**

合法用户的非授权访问是指合法用户在没有得到许可的情况下访问了他本不该访问的资源。一般来说，每个主机系统中，有一部分信息是可以对外开放的，而有些信息是要求保密或具有一定的隐私性。外部用户（指外部系统或网络合法用户）被允许正常访问一定的信息，但他同时通过一些手段越权访问了别人不允许他访问的信息，因此造成他人的信息泄密。所以，还得加强访问控制的机制，对服务及访问权限进行严格控制。

**3、防范假冒合法用户的非法访问**

从管理上及实际需求上是要求合法用户可正常访问被许可的资源。既然合法用户可以访问资源。那么，入侵者便会假冒合法用户的IP地址或用户名等资源进行非法访问。因此，必需从访问控制上做到防止假冒的用户访问。

#### 安全审计及日志管理

**1、安全审计**

审计是对网络上和系统中，与安全有关的重要活动进行监控、识别、记录、报警、响应的安全产品。它是能够提供更高应用层次、更高智能的安全手段。如今的网络和计算机系统虽然已经采用了一些安全防范措施，但仍然需要安全检测和审计产品，对重要的网上活动进行监视和记录，这样一旦系统瘫痪或者被入侵就能够进行侦破和取证，并能够发现安全防范系统的不足，加以改进。

安全审计系统可以对安全产品（如防火墙，IDS、AV等）、网络产品（如router、SWitch）、应用系统（如Web、 Mail）、操作系统（如Windows、 Linux、Unix）等产品和系统的日志信息统一进行收集并集中存储，同时采用先进的技术进行综合分析，检测出网络和系统中的安全隐患，以报警和直观的、可视化的方式显示出来，便于及时发现安全漏洞，采取有效措施，提高安全成效。

审计系统根据实际需要还会提供一些特殊的功能，如自学习、地址分析、服务类型分析、报文长度分析、流量分析、报文内容分析等智能分析模块。这些附加功能可以进一步满足计算机网络系统的特殊需要。

**2、日志管理**

系统要有完善的日志功能，保证操作员的每一笔操作都有据可查，记载任何进入系统的行为，包括对重要数据的修改情况，监测系统的运行，保证在数据发生问题时有据可查，避免个别人员的营私、舞弊行为。

对操作员的每一步操作都做日志记载。日志内容包括：哪个操作员、对哪个模块进行了什么操作，以及对一些重要数据表的操作前、操作后变化的记录，同时有日志查询功能，可以按用户要求对日志进行查询。

根据日志的功能，将日志分为功能日志和系统日志两类，下面将详细说明：

功能日志及实现

功能日志是指系统必须保存的，对系统中一些重要操作的记录。日志中需要记录操作人员、操作时间、操作的功能模块名称以及用户所执行的操作等等信息。记录和跟踪各种系统状态的变化，如提供对系统故意入侵行为的记录和对系统安全功能违反的记录。实现对各种安全事故的定位，如监控和捕捉各种安全事件，记录发生时间、发生地点和事件类型。同时，对于功能日志，同样要实现对日志的记录和查询功能。

对于功能日志，使用数据库来保存，并提供公共的API接口来实现日志的记录和查询功能。在每一个业务实现的时候，需要调用功能日志的API接口来添加功能日志。

系统日志及实现

系统日志主要用来记录程序的调试信息、启动和初始化状态、出错信息等；系统日志记录可以动态的记录在各种存储介质中，比如日志文件、数据库或者显示在控制台上等等。将系统日志分为三个等级，分别是DEBUG级别、INFO级别和ERROR级别。

DEBUG级别详细的记录程序的调试信息。该级别在调试程序时使用。

INFO级别详细的记录系统启动时的信息以及一些重要属性的加载信息。一般用在系统初始化和一些重要的属性初始化时使用。

ERROR级别详细的描述程序的出错信息和程序中捕获到的违例信息。用在出错和违例捕获时。

这三个级别的顺序是：ERROR > INFO > DEBUG。系统日志可以动态的调整需要记录的等级，比如：如果选择使用INFO级别，则日志文件中不会记录DEBUG级别的日志，而只记录INFO和ERROR级别的日志。

#### 权限管理

权限管理采用集中授权的工作模式，提供系统内的资源管理、用户角色定义和划分、权限分配和管理、权限认证等功能。权限管理主要是由管理员进行资源分类配置、用户角色定义及授权等操作；权限认证主要是根据用户身份对其进行权限判断，以决定该用户是否具有访问相应资源的权限。

权限管理与统一认证相结合，为基础地理数据及数据服务平台项目提供方便、简单的、可靠的授权服务，从而对内网用户进行整体的、有效的访问控制，保护系统内的资源不被非法或越权访问，防止信息泄漏。

权限管理应与统一认证相结合，由统一认证进行严格的身份认证，保证用户身份的真实性。

权限管理采用基于角色的访问控制策略，能够对用户和角色进行灵活授权。在定义角色时，可以采用职称、职务、部门等多种形式，灵活反映各种业务模式的管理需求。

#### 密码技术

密码服务应提供加解密、签名及签名验证、数字信封封装及解封等安全服务，以支持信息的保密性、完整性、真实性和不可抵赖性。客户端的密码服务由实体鉴别器提供，服务器端由加密服务器提供。密码服务系统要构建一个相对独立的可信计算环境。所有密码算法必须在经国家密码主管部门审批的密码设备上运行。

密码服务单元的密码算法采用国家密码主管部门审核批准的算法，密码算法由国家密码主管部门审核批准的专用密码设备实现，密钥运算都在密码硬件内实现。密钥加密存储在安全载体中或者密码服务系统的密码部件中，不以明文暴露在系统外。安全载体采用国家密码主管部门审核批准的安全载体。密码服务具有以下功能：

数据加解密的运算功能：提供对数据的加密和解密等运算功能，包括对称加解密，非对称加解密运算；

数据摘要和完整性验证：提供对数据进行摘要运算功能，并具有验证数据完整性功能。能够实现数字摘要算法功能，提供对数据进行摘要运算和验证摘要的功能；

数字签名和签名验证的运算功能，提供对数据的签名和签名验证等运算功能；

数字信封，提供对数据的数字信封（包括多证书的数字信封）封装和解封装等运算功能；

会话密钥生成和存储功能：提供指定长度的随机数功能，可以作为对称密钥和会话密钥；

提供对多密码算法的支持，用户根据国家密码主管部门的要求可以灵活地选择并配置合适的密码算法。

分布式计算功能，采用分布式计算技术，随着业务量的增加，灵活增加密码服务模块，实现性能动态按需平滑扩展，且不影响上层应用系统。

#### Web安全防护

对web安全防护将采用以下三种措施进行防范：

**1、利用IDS对SQL注入和跨站攻击进行实时监控，由防火墙进行阻断。**

**2、在Web服务器前部署Web应用防火墙，来防范来自应用层的风险。**

Web应用防火墙代表了一类新兴的信息安全技术，用以解决诸如防火墙一类传统设备束手无策的Web应用层安全问题。与传统防火墙不同，WAF工作在应用层，因此对Web应用防护具有先天的技术优势。基于对Web应用业务和逻辑的深刻理解，WAF对来自Web应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站站点进行有效防护。

**3、通过在重要Web服务器安装网站防篡改软件，实现对Web页面的保护。**

Web网页防篡改系统通过服务器文件访问底层驱动技术，对保护的对象（静态网页、动态执行脚本、文件夹）实时监测其属性，一旦发现更改立刻阻断非法篡改操作，阻止网页文件被修改，并实时通知管理客户端，如果发生文件篡改现象，系统也会自动从可信端进行恢复，彻底地保证了网页内容不被篡改。

#### 数据安全

**1、数据传输安全**

根据综合救灾减灾应急指挥业务特点，设计相应的数据传输策略以保证数据传输安全，主要包括：

关键业务数据传输安全：提供HTTPS的访问机制，采用SSL加速器解决访问性能；

批量数据传输安全：基于依据统一标准和规范构建数据交换平台以批量报文的方式完成机构之间的数据交换。对于异步数据传输，通过消息队列的数据恢复机制保证数据零丢失；

局域网内服务器和服务器之间的数据传输安全：采用SSH协议进行安全传输；

应急工作人员远程办公的安全访问：通过IP加密机接入业务专网。IP加密机最大的好处之一就是不需要安装客户端程序，远程用户可以随时随地从任何浏览器上安全的接入到内部网络，安全地访问应用程序，因此降低了管理员维护客户端的成本。利用IP加密机可实现：用户身份认证，防止外部人员非法接入，同时能够通过加密，保护在互联网上传输数据的安全。基于安全性的考虑，IP加密机设备部署在互联网接入区的防火墙的DMZ区。

**2、数据备份与恢复**

建立完整的冗余和备份策略。对于重要的网络节点和设备都应当实现冗余。备份包括本地、异地、实时等方式，也要根据每天、每周、每月等要求分别设定不同的备份内容和要求。

利用异地灾难备份中心，实现异地实时备份功能。

### 终端安全设计

**1、防病毒**

桌面的病毒防范可以利用现有防病毒系统进行安全防护。整个局域网需要统一使用网络版的病毒防护系统，便于升级和管理。针对恶意软件和ARP、蠕虫等网络病毒可以采用辅助工具来完成。

安装并开启个人防火墙，防止非法入侵计算机终端。

**2、计算机准入控制**

通过安全策略的制定，利用交换机的802.1x协议，实现设备准入控制。外来计算机接入局域网之前，要访问事先设置的修复服务器，符合修复服务器设置的安全策略后方可接入局域网，否则将对外来计算机进行修复。

通过桌面管理系统的准入控制功能实现安全准入管理。

**3、计算机的非法外连的管理**

对于内网的计算机，须杜绝私接设备访问互联网的情况。对于私自访问互联网的行为，系统管理员可以及时得到报警信息，便于管理员及时处理；对于该行为，可以通过系统向该违规用户发送告警信息，让该用户主动切断互联网连接，或采取中断互联网连接的策略，使其连接过程失效；

同时利用802.1x协议，对该计算机进行断网处理，使其无法访问局域网。

**4、USB设备管理**

由于客户端数据交换主要通过网络或USB设备进行拷贝，因此需要对USB设备进行细化管理，可以自动识别、控制接入的USB设备类型，控制USB设备的读写权限、读写方向，并对USB操作进行记录和审计，提高了客户端的安全性。同时配合802.1x协议，对违规计算机进行报警或断网处理。

**5、实名制管理**

通过实名制管理，可以绑定计算机与使用人，一旦出现问题，有利于快速定位并及时解决。同时配合802.1x协议，对违规计算机进行报警或断网处理。

**6、补丁管理**

实现自动化的分发系统安全补丁，提高整个网络的系统安全。同时配合802.1x协议，对不符合要求的计算机进行报警或断网处理。

**7、系统日常维护管理**

主要实现对终端电脑的统一的运行、维护管理，提高运行维护效率。包括：软/硬件信息自动收集管理，远程在线帮助，应用软件的统一分发、部署、升级等。

### 系统层安全设计

主机（系统）层的安全设计主要从操作系统和数据库两个方面来考虑。根据等级保护三级的防护要求，主要从以下几个方面对主机的安全进行防护：

**1、身份鉴别**

对登录操作系统和数据库系统的用户进行身份标识和鉴别，杜绝默认帐号，不合规则的帐号登录访问；操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施，三次登录失败帐号会被锁定。为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。

对服务器进行远程管理需要采用安全的模式，针对系统管理员除用户名和密码外，还需要采用数字证书或者UKEY等其他身份鉴别手段。

**2、访问控制**

建立标记规则，在服务器等实体资产上粘贴属性标签，文档介质类粘贴或打印密级等标记，对于电子数据使用文件名或文件注释进行标记。建立访问控制策略，依据最小原则授予用户权限，操作系统和数据库系统要使用不同的特权用户，对用户权限分配应当定期检查。

严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；及时删除多余的、过期的帐户，避免共享帐户的存在。

**3、安全审计**

由于开启操作系统和数据库的审计功能会影响系统的性能，建议在核心交换安全域配置主机数据库综合审计系统，以便于对主机和数据库信息进行审计。

**4、入侵防范**

部署主机防火墙设备或者主机防病毒软件中的入侵检测模块，监视外来的入侵行为并记录，定期进行系统升级和安全加固。

**5、恶意代码防范**

在主机上安装防病毒产品。

**6、资源控制**

Windows系统通过本地安全策略限制登录IP，Unix系统可通过TCP Wrapper工具进行访问IP限制。使用监控管理软件对服务器的CPU、硬盘、内存、网络等资源的使用情况进行监视，设置系统资源过低报警的门限值。

数据库系统安全

由于院地理信息中心的大多数服务目标是社会各界用户，并且数据来自很多方面，所以数据库的安全至关重要。数据库的安全保密的解决措施主要有以下几点：①加固数据库安全，及时打上安全补丁；

②系统管理员为数据库使用人员分配特定的账号

和密码，对“所有者”、“组”、“其他”三项内容设置严密

的权限；

③制订完善的口令策略；

④修改系统参数，限制对权限、角色、堆栈等内容

的调用；

（3）防病毒系统

目前市场上的各类防病毒软件产品功能已经非常完善，但是在整体病毒防护上，建议采用网关级硬件防火墙，这样可以保证整体的安全性，并提供中心全部网络范围的病毒防护。芜湖市勘测院地理信息中心的具体方案是：使用网神SecGate 3600-F3硬件防火墙和McAfee杀毒软件，建立以Windows2003为控制中心的管理模式，将病毒库升级的工作交给控制中心的

McAfee防病毒中心来做。

### 网络层安全设计

利用现有网络及安全设备，保证应急指挥平台系统的网络、数据、信息安全，政务机房既有防火墙、IPSEC VPN、SSL VPN、带宽管理、防病毒、入

侵防御、内容过滤等多种安全功能，并有网络杀毒软件，及时更新病毒库，时保障网络对最新病毒的查杀。

### 物理层安全设计

这里说的物理层安全指的是物理连接方面的安全，尤其是指不同密级之间的网络连接规范和要求，保证物理结构上的安全。主要包括以下几个内容：

（1）电力中断防护由于院地理信息中心拥有大量的设备，如网络设备、服务器、输入输出设备（扫描仪、打印机）、个人电脑等。所以电力供应非常重要，应准备两种不同源的电路，重要设备均要有双电源冗余设计。

（2）恶意的物理破坏防范

采用网管设备和监控系统对机房、档案库、重要设备以及出入口进行监视保护。办公地点采用门禁系统，利用身份卡进出人员身份的识别（有条件的单位可以采用指纹识别，如武汉市勘测设计研究院基础地理信息中心），防范外部人员的随意进入。对于作业人员的个人办公电脑，完全杜绝输入功能，以免从外部感染病毒或间谍程序。原则上不允许安装光软驱，已经安装的必须屏蔽；对BIOS设置密码，限制USB等输入接口的使用；不允许随意拆机，在网线水晶头、机箱锁等关键部位粘贴易碎标签，安排专人定期检查，一旦发现问题，及时上报院领导。设置专门的输出终端，专人管理，所有输出的数据必须经过审核，在指定的终端进行输出。

（3）电磁泄露保护

对于重要的，涉密的设备进行电磁泄露保护。

（4）安全旁路问题

安全旁路问题主要是限制和管理采用物理隔离的内部网络的人员拨号行为。

（5）设计安全拓扑结构

针对地理信息中心的运行网络环境，存在涉密网络与非涉密网络间的连接，也有内、外网的连接，拓扑结构复杂。应采取物理隔离方式，实行完全网络上的隔离，对于涉密网与非涉密网之间的连接，无设备相连。原则上办公单位与数据中心的连接均用防火墙进行逻辑隔离，保证可信的数据传输及对非法访问的拒绝。院内部网络的安全拓扑结构图所示。

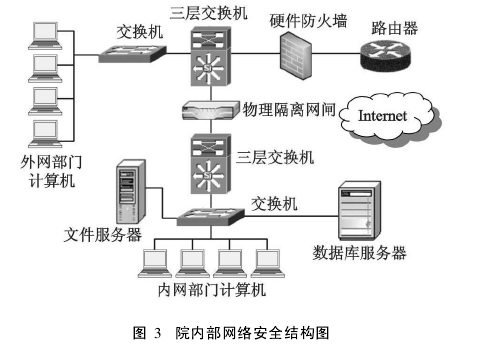


图14.5-2网络安全拓扑结构图

10、备份系统设计

集中式数据级备份

采用高性能、一体化和节能的备份设备，可支持异构平台环境的集中备份和恢复管理，内置的虚拟介质池功能，使设备具有容量与处理性能呈线性增长的特性，可满足大规模的备份需求。

**统一保护**：针对Windows服务器环境、Linux服务器环境、Unix服务器环境以及PC桌面环境，可提供集中统一的备份和恢复管理。

**全面保护：**提供操作系统、应用系统和文件数据三层全面保护，应用系统支持 SQL Server、Oracle、Sybase、Exchange Server、Lotus Domino、DB2、MySQL、Active Directory等几乎所有主流应用，无论是数据破坏，还是业务系统损坏，都可得到完整地恢复。

方案一中应用到集中式数据备份，其原理就是采用 IP SAN备份软件  对两幢楼中的SAN 数据进行 Disk-Disk 集中式备份。系统将在大楼-A 内配置一台备份服务器，用来统一管理两幢大楼中所有服务器的数据备份与恢复，备份的数据不仅要保存在同一楼内，同时还要保存到另一楼内一份，以做异地备份，而所有的这些备份操作全部是通过备份服务器来进行统一设置，这样不仅满足了用户的需求，而且方便了管理员的操作。

**拓朴结构**

拓扑图如下

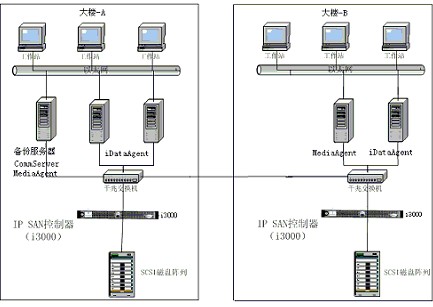
[](http://img.watchstor.com/uploadimg/20100326/1851300.jpg)

图  9-8  系统方案一拓扑图   系统架构：

采用两台IP SAN备份网络存储服务器连接 1T RAID 作为备份介质，用一台服务器（或普通的 PC 机）作为备份/介质管理服务器，其他需要备份的应用服务器上安装相应的代理客户端，作为备份客户端。通过网络和其他服务器连接构成集中备份网络。

备份恢复说明：该系统采用集中备份/恢复/监控的方式。由中心管理员制定备份数据的备份任务策略和数据存储策率。每台备份客户端的代理程序根据相应的备份任务，将相应的数据备份到备份服务器上的 RAID 中。到进行数据恢复时，则每台客户端的代理程序将从备份服务器上的介质中将相应的数据恢复到指定的区域。

以上过程都可在线进行。 数据存放：该系统支持数据的分散存放和多拷贝，备份数据即能存放在本地的 RAID中，也能存放到异地的磁盘上，或者是离线的归档设备上（LTO 带库）等。同时所有的备份数据集都包含元数据和备份数据。因此能保证数据恢复的快速，准确，安全（多分拷贝），可靠（数据恢复时不必访问元数据库）。

用户管理：该系统采用多用户和群组的管理方式，可以采用自主备份的模式，能设定份权限和优先级。增加了备份的安全性，减少了集中管理人员的负担。 日志传送：该系统可以在 WAN 网络上进行数据传送时，支持日志传送方式。这样不仅保证了备份任务的完整性和可靠性，也降低了对网络资源的浪费。

当网络发生故障时，可以自动从故障点继续备份。（断点续传）技术特点 采用 Disk-Disk 备份方式：磁盘到磁盘的备份方式，提高了备份速度（顺序读写比 LTO磁带快 3 到5 倍），减少了备份窗口，加快了备份速度。

支持异地灾备模式：系统支持一份备份数据多份拷贝，这就可以利用 IP SAN备份方便的将备份数据保存到异地去，以防止本地环境出现大范围的自然灾害而造成数据的丢失。 支持 OnePath Restor 恢复和数据合并模式（将增量备份和全备份合并成全备份）：这样就减少了全备份的时间，加快了恢复的速度（不必恢复多次，比其他应用恢复速度快 1 倍以  
上）。

（特有功能） 支持备份任务的断点续传：这样保证了即使备份期间发生故障，也能从该故障点继续备份，而不必重新备份。 支持应用级的 SnapShot 备份和 QR 快速恢复:可以不必重新安装应用，就可重启应用，加快应用恢复速度。 支持 AD 和 Exchange的记录级备份:这样能对单个属性和信息进行备份和恢复。这样如果某些内容不对，只要恢复部分数据即可。而不必进行所有数据的恢复，加快了恢复速度。

（特有功能） 采用日志方式在网上传送数据:保证了备份数据的完整性，节约了网络带宽。（特有功能） 系统具有很好的可扩展性：无论是备份介质还是备份机器，无需任何设置，直接接入网  
络就能工作。 系统支持所有的主流平台和操作系统平台，也支持所有的备份介质（Disk/Tape ..）。

采用文件系统作为备份数据集：符合操作人员习惯，便于数据迁移和升级。 采用集中单点管理，支持异地的 WEB监控和管理：能方便的监控所有的备份资源和备份数据集。支持用户和群组管理模式：使得备份管理可以由用户自主管理，减少了中心管理员的压力。

支持基于存储策率的备份模式：由管理员制定统一的数据迁移模式，当备份存储策率改变时，不用一一修改所有的备份任务。 采用 BackupStorageSet 模式：支持备份数据集的分布放置和不同存储方式。使得数据监控一目了然。