论网络管理

摘要：

信息化建设在提高医院管理的科学性、方便患者就医等方面发挥了重要的作用。网络建设是医院信息化建设的基础内容，网络管理水平的高低直接决定了医院的信息化建设水平。活动目录是 Windows 系统网络结构中的重要组成部分，是实现网络管理规范化的基础。本文为了解决解决当前医院信息化建设中网络管理所面临的突出问题，应用 Windows 活动目录对医院网络内的客户端和用户进行规划组织，通过设置用户类型、下发组策略等方式对医院网络内客户端和用户进行灵活地配置管理。应用活动目录可对医院网络内客户端和用户进行统一、灵活、安全的管理。从而提高了对医院网络的管理水平，具有广阔的应用前景。

正文：

***军第**医院与于 2008 年开始医院信息化建设，信息化建设旨在提高医院管理的科学性、方便患者就医。该项目主要是建设覆盖全院的基础网络、将医院就医、划价、开方、支付、结算、报账等流程计算机化。同时建设过程中注意系统的安全性和外界的交换性。同时考虑有效组织网络资源，提高办公效率，节省网络运营成本，提高网络的利用率、通用性和安全性。我为**军第**医院信息化建设的项目经理，主要负责该项目的建设和用户的沟通工作。

目前， ***军第**医院是 310 指挥网、综合信息网、远程医学网和内部局域网等多个网络并存，并且各个网络之间物理隔离。其中，310 指挥网、综合信息网、远程医学网有其特定的应用范围，终端数量少，维护工作量也较小。内部局域网主要实现医院内部的信息共享，医院的大部分日常工作都是在内部局域网上完成的。由于客户端使用环境和用户操作水平的参差不齐，医院网络管理的主要工作就是对内部局域网和网络内客户端的管理。

1. 医院网络管理面临的问题

结合日常工作实践，医院网络管理面临的主要问题有以下几个方面：

（1）网络内客户端设备的日常维护工作繁重。网络内客户端设备有以下几个特点：一

是数量多，一个中等规模的医院客户端设备往往都有数百或上千台。二是类型杂，客户端设备包括有计算机、打印机、扫描仪、医疗终端等设备，某一种设备又有多种不同的型号，某一种型号的设备又安装了不同的操作系统、应用软件等。三是客户端设备地址位置分散，分布在全院各个科室部门。如果对这些客户端设备管理不当，就会为日常维护工作带来了很大的困难。

（2）网络内用户的有意或无意的违规操作。用户在使用终端设备进行日常工作时，由于操作水平有限、安全意识淡薄等原因，对终端设备可能会进行有意或无意的违规操作。例如，用户由于对计算机操作系统不了解，进行一些错误或非法操作导致系统不能正常使用；用户随意使用移动存储设备拷贝文件、安装程序等，很可能使网络内计算机感染各种病毒，并对整个网络安全构成威胁。

（3）网络内存在的安全隐患。网络系统可能存在的安全隐患大体可分为以下几种：一是网络设备安全隐患，网络路由器、交换机可能存在安全漏洞或“系统陷门”；二是操作系统安全隐患，目前流行的多种操作系统都存在不同程度的网络安全漏洞；三是网络用户安全隐患，来自网络内部用户有意或无意的安全威胁，如操作员安全配置不当造成的安全漏洞，用户安全意识不强等都会对网络安全带来威胁；四是应用服务安全隐患，许多应用服务系统在访问控制及安全通信方面考虑较少，如果系统设置错误，很容易造成损失。

2．应用活动目录加强医院网络管理技术方案

医院网络主要实现了两方面的功能：

·医院职能管理通过运行各种查询与统计系统和网站系统实现对医院的职能管理。

·医疗业务管理。通过运行医生工作站、护士工作站、挂号计费等系统实现对医院医疗业务的管理。应用活动目录可以实现对医院网络的统一、灵活、安全管理，大大减轻日常网络管理和维护的压力。

我院的内部局域网络根据地理位置分为门诊楼、住院楼、机关办公区和传染病区 4 个子局域网络，它们之间通过光纤汇聚在主控机房的中心交换机，连接成医院局域网络。由于医院网络内仅有终端设备数百台，因此 1 个活动目录域已完全能满足需求，设置医院网络域名为 322yy.com。医院网络的活动目录结构形式要尽量体现医院的组织形式和功能需求，同时又要方便网络管理。域包括医院机关、临床科室、门诊科室、辅诊科室、服务器组等组织单

元，各组织单元包括相应科室部门的用户账号、计算机和共享资源等信息。域控制器设在主控机房内，并将其配置为 DNS 服务器，以提高用户登录系统时的响应速度。

（1）限制域用户权限。

要合理规划分配好域内用户的操作权限，在分配用户权限时，遵循最低权限原则。对于域内的普通用户，都可将其添加到 Domain Users 用户组中。Domain Users 用户组对系统的操作权限很低，它不能添加、删除硬件设备，不能安装、卸载应用程序，不能设置共享，不能启动或停止系统服务，不能修改系统目录和注册表，甚至不能修改系统时间，只能运行一些已安装的应用程序和进行基本的文件操作。这样，可以大大降低用户由于误操作对系统或网络的影响，加强医院网络的安全性和易管理性。

（2）统一配置域用户环境。

在活动目录中，可以通过配置组策略对用户的桌面、墙纸、屏保、开始程序、控制面板等进行统一配置管理。管理员在主控机房内即可方便地对这些用户环境进行统一配置，而不必到现场实地操作。例如，上级曾要求我单位机关计算机统一安装下发的保密墙纸和屏保程序。如果没用应用活动目录，需要到现场对每台计算机进行配置，工作量非常大。而应用活动目录后，只需要在相应组织单元中应用一个组策略即可轻松实现，大大减少了维护的工作量，方便对客户端进行统一、灵活的管理。

（3）应用好开机、关机、登录、注销脚本。

脚本是使用一种特定的描述性语言，依据一定格式编写的可执行文件，又称作宏或批处理文件。应用脚本可以通过编程的形式大大扩展组策略的功能，编辑脚本并将其应用到开机、关机、登录、注销过程中可以实现在多种状态下对客户端进行一般组策略无法实现的控制管理[5]。例如，我们要求客户端在登录时要自动映射某网络驱动器，就可以通过在组策略中添加登录脚本的方式实现。

（4）自动分发应用软件。

在日常工作中，经常会碰到给客户端安装各种应用软件的工作。应用组策略中的软件自动安装功能可以方便地实现多台客户端统一安装应用程序。需要注意的是，活动目录中默认只能安装 MSI 格式的安装包，对于其他格式的安装软件可以通过制作 ZAP 文件或第三方软件将其打包成 MSI 格式再进行软件发布。

（5）限制移动存储设备使用。

目前，移动存储设备由于经常拷贝各种文件，感染病毒的概率很大，如果任其在医院网络内计算机上随意使用，会给整个网络带来了很大的安全隐患。因此，我们对临床科室的计算机采用了限制移动存储设备使用的策略。尤其是对 USB 存储设备的限制使用，大大降低了计算机病毒感染的几率，同时又不影响其他 USB 终端设备（如 USB 接口打印机）的正常使用，方便对客户端进行安全管理。

（6）应用好计算机安全策略配置。

计算机的安全策略包括账户策略、本地策略、密码策略、公钥策略、IPSec 策略、事件日志、受限制的组、系统服务、注册表、文件系统等。要集中管理好用户账号，为特定的用户或组指派一定范围的管理任务，使其能控制设定本地资源。同时做好软件限制策略，控制可以在客户端计算机上运行的程序，以保护计算机不会受到不可信代码的攻击。正确配置审核策略，可以跟踪用户、操作系统活动的成功或失败事件，维护用户、操作系统的活动记录。

3．发现的问题和解决办法

在应用活动目录前要做好网络内域、组织单元、用户组、用户、计算机等的组织规划。首先要规划好整个系统的域结构，活动目录可包含一个或多个域，如果整个系统的目录结构规划得不好，就不能很好地发挥活动目录的优越性。其次，要对组织单元所应用的组策略和用户组、用户的使用权限做好规划，在保证正常使用的前提下，最大限度地加强网络的安全性。另外，还要做好对这些策略、权限的逆操作规则，不但能限制用户的某项操作，在有特定需要时又能解除此项限制，做到对用户和计算机的策略、权限收放自如。

在应用活动目录后要做好域控制器冗机备份，定期备份域控制器的系统信息。否则出现问题，整个网络就会瘫痪。

4．小结

活动目录是 Windows 分布式网络体系结构的基础。应用活动目录来进行医院网络的维护管理，能够实现网络资源和用户的集中管理，既能对网络资源和用户进行统一的管理配置，又能灵活地对有特殊需求的用户进行个性管理，同时又能增强医院网络的安全性。