项目 3
域和活动目录的管理

项目学习目标

(1) 了解活动目录的概念及功能。
(2) 掌握域、域树、域目录林、组织单位的概念。
(3) 掌握域控制器的安装与设置。
(4) 掌握额外的域控制器的安装与设置。
(5) 掌握子域控制器的安装与设置。
(6) 掌握将服务器三种角色相互转换的方法。
(7) 掌握客户端登录域的方法。

3.1 项目提出

某上市公司的企业内部网原来一直采用“工作组”的网络资源管理模式,随着公司的快速发展,企业内部网的规模也在不断地扩大,覆盖了 5 栋办公大楼,涉及 1000 多个信息点,还拥有各类服务器 30 余台。

由于各种网络和硬件设备分布在不同的办公大楼和楼层,网络的资源和权限管理非常复杂,产生的问题也非常多,管理员经常疲于处理各类网络问题。那么,是否有办法减少管理员的工作量,实现用户账户、软件、网络的统一管理和控制呢? 例如,能否实现用户在访问网络资源时只需登录一次即可访问不同服务器上的网络资源?

3.2 项目分析

在“工作组”模式下,公司的员工要访问每台服务器,则管理员需要在每台服务器上分别为每个员工建立一个账户(共 $M \times N$ 个,M 为服务器的数量,N 为员工的数量),用户则需要在每台服务器中(共 M 台)登录。

在“域”工作模式下,若服务器和用户的计算机都在同一个域中,用户在域中只需要拥有一个账户,用该账户登录后即取得一个身份,便可访问域中任意一台服务器上的资源。每台存放资源的服务器并不需要为每位用户创建账户,而只需要把资源的访问权限分配给用户在域中的账户即可。因此,用户只需要在域中拥有一个域账户,并只需要在域中登录一次即可访问域中的资源。

将基于工作组的网络升级为基于域的网络，需要将一台或多台计算机升级为域控制器，并将其他所有计算机加入域成为成员服务器或域中的客户端。同时将原来的本地用户账户和组也升级为域用户和组进行管理。活动目录是域的核心，通过活动目录可以将网络中各种完全不同的对象以相同的方式组织到一起。活动目录不但更有利于网络管理员对网络的集中管理，方便用户查找对象，也使得网络的安全性大大增强。

3.3　相关知识点

3.3.1　工作组概述

我们组建局域网的目的就是要实现资源的共享，而随着网络规模的扩大及应用的需要，共享的资源就会逐渐增多，如何管理这些在不同机器上的网络资源呢？工作组和域就是在这样的环境中产生的两种不同的网络资源管理模式。

工作组(Workgroup)就是将不同的计算机按功能分别列入不同的组中，以方便用户管理。在一个网络内，可能有成百上千台工作的计算机，如果不对这些计算机进行分组，而是都列在“网上邻居”内，可想而知会有多么乱。为了解决这一问题，Windows 引用了“工作组”这个概念。例如，一个公司会分为诸如行政部、市场部、技术部等几个部门，然后行政部的计算机全都列入行政部的工作组中，市场部的计算机全部都列入市场部的工作组中。如果要访问其他部门的网络资源，就通过“网上邻居”找到那个部门的工作组名，双击进入就可以看到其他部门的计算机了。

在安装 Windows 系统时，工作组名一般使用默认的 Workgroup，也可以任意起个名字。相对而言，位于同一个工作组内的成员相互交换信息的频率最高，所以用户进入“网上邻居”时，首先看到的是其所在工作组的成员。如果要访问其他工作组的成员，需要双击“整个网络”，才会看到网络上其他的工作组，然后双击其他工作组的名称，这样才可以看到里面的成员与之实现资源交换。

除此之外，也可以退出某个工作组，方法也很简单，只要将工作组名称改变一下即可。不过其他人仍然可以访问你的共享资源，只不过你所在的工作组名发生改变而已，因此工作组名并没有太多的实际意义。也就是说，用户可以随时加入同一网络上的任何工作组，也可以随时离开一个工作组。“工作组”就像一个自由加入和退出的俱乐部一样，它本身的作用仅仅是提供一个“房间”，以方便网上计算机共享资源的浏览。

工作组是最简单的网络资源管理模式。对工作组中的计算机没有统一的管理机制，每台计算机的管理员只能管理本地计算机，例如，对本地计算机的安全策略进行设置，对本地连接和共享进行管理等。

在账户的管理上，工作组也没有统一的身份验证机制，用户只能使用计算机的本地账户登录该计算机，并由本地计算机对用户的身份进行验证，当对网络上的共享资源进行访问时，必须提供访问共享资源的凭据，因此，用户需要记下访问不同服务器的账户和密码。

工作组中的计算机没有统一的对网络资源进行查找的机制，例如，对网络中的共享打印机、用户账户信息以及共享文件夹的查找。

由此可见，工作组的网络资源管理模式存在诸多限制，因此，这种形式仅适用于网络规

模较小的应用中。当企业规模不断增大、计算机数量不断增多时,需要有统一的管理机制,对用户账户、共享资源等进行统一的管理。此时,工作组的网络资源管理模式不再适合了。

在 Windows Server 2008 系统中要启用"网络发现"功能后,才可以找到网络中的任何"邻居"主机,以及被其他的"邻居"主机所发现。如果这样还不能从网络中寻找到"邻居"主机,那么就有必要检查一下 Windows Server 2008 系统中是否启用了"Microsoft 网络的文件和打印机共享"功能组件,如图 3-1 所示。

此外,还需要检查 TCP/IP 属性参数是否设置正确,以保证 Windows Server 2008 系统主机的 IP 地址,与要寻找的"邻居"主机的 IP 地址处于同一个网段。

如果仍然还不能从网络中寻找到"邻居"主机,可以检查与系统相关的 Computer Browser 服务信息,其操作步骤如下:选择"开始"→"运行"命令,在打开的"运行"对话框中输入 services.msc 命令,单击"确定"按钮后,打开"服务"窗口。找到并双击 Computer Browser 系统服务,打开如图 3-2 所示的"Computer Browser 的属性(本地计算机)"对话框。设置该服务的"启动类型"为"自动",单击"应用"按钮,然后单击"启动"按钮,将该服务的状态设置为"已启动"。还应及时检查 Computer Browser 系统服务所依赖的另外两个系统服务 Workstation 和 Server 是否正常运行,这两个系统服务提供了最基本的网络访问支持。

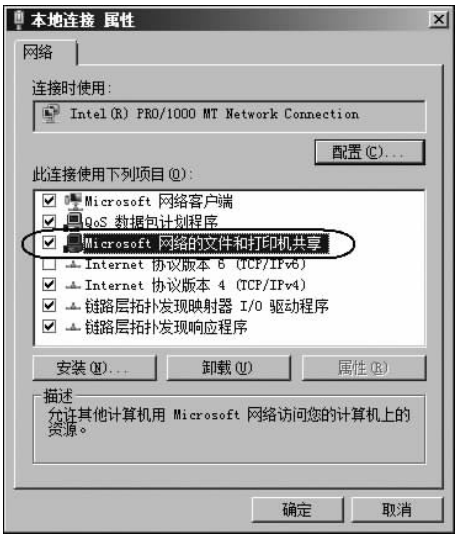

图 3-1　启用文件和打印机共享

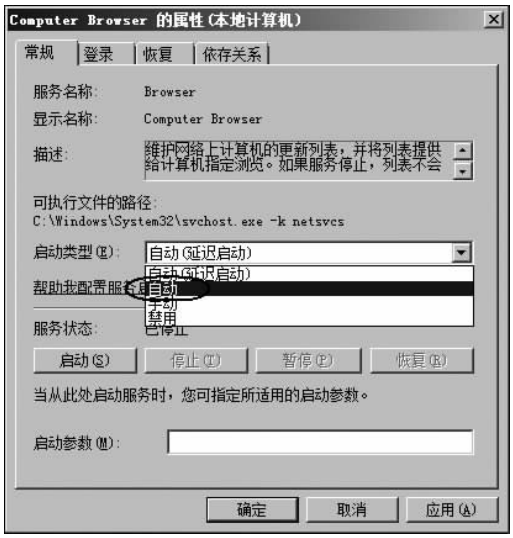

图 3-2　启用 Computer Browser 服务

3.3.2　目录服务和活动目录

目录是一个数据库,存储了网络资源相关信息,包括资源的位置、管理等。目录服务是一种网络服务,用来标记管理一个较为复杂的网络环境中的所有实体资源(如计算机、用户、打印机、文件、应用程序等)。实际上,目录服务既是一种信息查询工具,如用来查询信息;又是一种管理工具,如用于网络资源管理,各种资源都可作为目录对象来管理,随着网络中对象数量的增长,目录服务变得越来越重要。

活动目录(Active Directory,AD)是一种目录服务,它存储有关网络对象(如用户、组、计算机、共享资源、打印机和联系人等)的信息,并将结构化数据存储作为目录信息逻辑和分层

组织的基础，以便管理员比较方便地查找并使用这些网络信息。活动目录实际上就是一个特殊的数据库，不过该数据库和以往大家接触到的 SQL Server 等关系型数据库有很大的差别。

活动目录是在 Windows 2000 Server 中推出的新技术，它最大的突破性和成功之一也就在于它全新引入了活动目录服务（AD Directory Service），使 Windows 2000 Server 与 Internet 上的各项服务和协议的联系更加紧密。通过在 Windows 2000 Server 的基础上进一步扩展，Windows Server 2003 提高了活动目录的多功能性、可管理性及可靠性。

在 Windows Server 2008 中，活动目录服务有了一个新的名称：Active Directory Domain Service（AD DS）。名称的改变意味着微软对 Windows Server 2008 的活动目录进行了较大的调整，增加了功能强大的新特性，例如新增了只读域控制器（RODC）、更新的活动目录域服务安装向导、可重启的活动目录域服务、快照查看以及增强的 Ntdsutil 命令等，并且对原有特性进行了增强。

活动目录并不是 Windows Server 2008 中必须安装的组件，并且其运行时占用系统资源较多。设置活动目录的主要目的就是提供目录服务功能，使网络管理更简便，安全性更高。另外，活动目录的结构比较复杂，适用于用户或者网络资源较多的环境。

“目录服务”与 Windows 系统中的“文件夹目录”以及 DOS 下的“目录”在含义上完全不同。活动目录是指网络中用户以及各种资源在网络中的具体位置及调用和管理方式，就是把原来固定的资源存储层次关系与网络管理以及用户调用关联起来，从而提高了网络资源的使用效率。

3.3.3　活动目录的逻辑结构

活动目录结构主要是指网络中所有用户、计算机以及其他网络资源的层次关系，就像一个大型仓库中分出若干个小储藏间，每个小储藏间分别用来存放不同的东西。通常情况下，活动目录的结构可以分为逻辑结构和物理结构，分别包含不同的对象，了解这些也是用户理解和应用活动目录的重要一步。

活动目录的逻辑结构非常灵活，它为活动目录提供了完全的树状层次结构视图，为用户和管理员查找、定位对象提供了极大的方便。活动目录的逻辑结构可以和公司的组织机构框图结合起来，通过对资源进行逻辑组织，使用户可以通过名称而不是通过物理位置来查找资源，并且使网络的物理结构对用户来说是透明的。

活动目录的逻辑结构按自上而下的顺序分，依次为林→域树→域→组织单元，如图 3-3 所示。在实际应用中，则通常按自下而上的方法来设计活动目录的逻辑结构。

1. 域

域（Domain）是在 Windows Server 2008 网络环境中组建客户机/服务器（C/S）网络的实现方式。所谓域，是由网络管理员定义的一组计算机集合，实际上就是一个网络。在这个网络中，至少有一台称为域控制器的计算机充当服务器角色。域控制器包含了由这个域的账户、密码及属于这个域的计算机等信息构成的数据库，即活动目录。管理员可以通过修改活动目录的配置来实现对网络的管理和控制，如管理员可以在活动目录中为每个用户创建域用户账号，使他们可登录域并访问域中的资源。同时，管理员也可以控制所有网络用户的行为，如控制用户能否登录、在什么时间登录、登录后能执行哪些操作等。而域中的客户计算机要访问域中的资源，则必须先加入域，并通过管理员为其创建的域用户账号登录域，才能

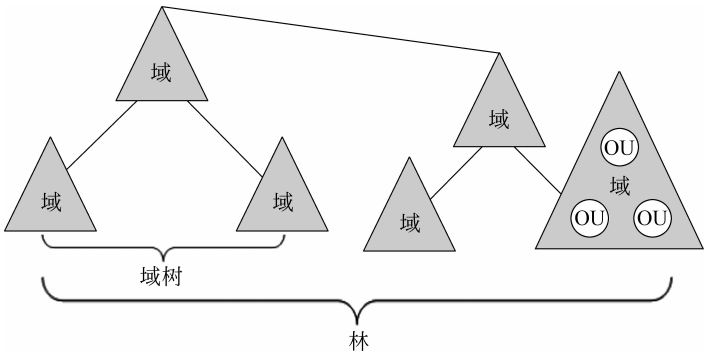

图 3-3　活动目录的逻辑结构

访问域中的资源,同时,也必须接受管理员的控制和管理。构建域后,管理员可以对整个网络实施集中控制和管理。

域(Domain)是 Windows Server 2008 活动目录逻辑结构的核心单元,是活动目录对象的容器。在 Windows Server 2008 的活动目录中,域用三角形来表示。

域定义了一个安全边界,域中所有的对象都保存在域中,都在这个安全的范围内接受统一的管理。同时每个域只保存属于本域的对象,所以域管理员只能管理本域。安全边界的作用就是保证域的管理者只能在该域内拥有必要的管理权限,如果要让一个域的管理员去管理其他域,除非管理者得到其他域的明确授权。

2. 组织单元

为了便于管理,往往将域再进一步划分成多个组织单元(Organization Unit,OU)。组织单元是一个容器,可包含用户、组、计算机、打印机等,甚至还可以包含其他的组织单元。组织单元不仅可以包含对象,而且可以进行策略设置和委派管理。

组织单元是活动目录中最小的管理单元。如果一个域中的对象数目非常多,可以用组织单元把一些具有相同管理要求的对象组织在一起,这样就可以实现分组管理了。而且作为域管理员,还可以指定某个用户去管理某个 OU,管理权限可视情况而定,这样可以减轻管理员的工作负担。

由于组织单元层次结构局限于域的内部,所以一个域中的组织单元层次结构与另一个域中的组织单元层次结构没有任何关系,就像是 Windows 资源管理器中位于不同目录下的文件一样,可以重名或重复。

在规划组织单元时,可以依据两个原则来进行:地理位置和部门职能。如果一个公司的域由北京、上海和广州三个地理位置组成,而且每个地理位置都有财务部、技术部和市场部三个部门,则可以按图 3-4 所示来规划组织单元。

在 Windows Server 2008 的活动目录中,组织单元用圆形来表示。

3. 域树

域树(Domain Tree)是由一组具有连续命名空间的域组成的。域树中的第一个域称为根域,同一域树中的其他域为子域,位于上层的域称为子域的父域。域树中的域虽有层次关系,但仅限于命名方式,并不表示对父域和子域具有管辖权限。域树中各域都是独立的管理个体,父域和子域的管理员是平等的。