MCSE（微软认证系统工程师）系列丛书

MCSE 试题详析大全

Microsoft Windows® 2000 Directory Services Infrastructure

考试必备
全国首套

Exam: 70-217

電子工業出版社

MCSE(Exam:70 – 217)

Microsoft Windows® 2000 Directory Services Infrastructure

试题详析大全

策　划:何学仪
主　编:钟　珞
副主编:李　辉　夏红霞
编　者:郑巧仙　赵广辉
　　许再哲　席守卿
　　孙　骏

电子工业出版社

Microsoft

Windows® 2000 Directory Services Infrastructure

试题详析大全

（光盘附书）

策　　划	何学仪
编　　著	东方激光工作室
责任编辑	董　娅　苏宁萍
出版发行	电子工业出版社　电子出版部
经　　销	各地新华书店
开　　本	1092 × 787mm　1/16
印　　张	35.5
标准盘号	ISBN 7 – 900074 – 12 – 0/TP·13

前 言

MCSE(Microsoft Certified Systems Engineer:微软认证系统工程师)是微软公司在我国推出的计算机高级技术人员认证考试之一,是全球公认的计算机软件高级人才认证,由比尔·盖茨签发的证书在全球 90 多个国家均得到承认。微软认证证书代表着企业及个人的技术实力,其拥有者在全球各地均可享有高就业机会、高薪、相关学业免学分的待遇,甚至在北美的一些国家可以作为外来移民的技术评估标准。

微软认证考试不同于一般的计算机普及考试,它的目的主要在于培养高级计算机专门人才。微软认证考试的内容科目具有很强的针对性,都是针对微软各个不同阶段的产品来进行考试的,产品升级了,考试的内容、题型甚至题量都相应地改变。Windows 2000 发布后,微软在 MCP(微软认证专家)以及 MCSE(微软认证系统工程师)认证策略上都有重大调整,所有考试的整体难度都有所增加,MCSE 难度比 NT 4.0 有一个大幅度的提高。

调整后的考试科目有很大变化,以前的考试只考 6 门,其中 4 门必考,两门选考。但 Windows 2000 系列考试科目有 7 门,具体分为 5 门核心课程和两门选考课程,没有参加过 Windows NT 4.0 考试的考生,必考以下 4 门课程:考试号 70 - 210,即微软 Windows 2000(专业版)安装配置与管理;考试号 70 - 215,即微软 Windows 2000(服务器版)安装配置与管理;考试号 70 - 216,即 Windows 2000 网络架构的实施与管理;考试号 70 - 217,即微软 Windows 2000 目录服务架构的实施与管理。

通过 Windows 2000 MCSE 的认证考核,技术人员将具有计算机网络系统方面的全面能力,包括设计、实现、维护和支持信息系统,在各种环境中使用 Windows 2000 Server 网络操作系统和 Net Enterprise Server 家族的服务器产品;加强、配置和管理复杂的 Internet/Intranet 解决方案;管理包含浏览器、代理服务器、主机服务器、数据库以及邮件和商业构件的系统;管理和分析站点。

Windows 2000 MCSE 就是在 Windows NT 4.0 的基础上升级而来的。Windows NT 4.0 考试在今年 2 月底已经停止,其证书的有效期最多可持续一年。

在此背景下,我们编写出版了 Windows 2000 MCSE 系统丛书,该套丛书具备以下特点,第一,它是国内第一套 Windows 2000 MCSE 考试复习用书,其体例独特,由“要点流程”、“重点综述”和“试题分析”组成,特别适合考生考试前的冲刺;第二,参考全真考试卷,编写了多套模拟试题,并给出参考答案,供考生做自测练习,以检查对考试内容的掌握程度;第三:考虑到中国人的思考习惯,本套丛书采用中文编写,让读者能更好地理解书中的内容。本书有配套光盘,其中包括书中全部“试题分析”和“模拟试题”,方便读者操作练习。光盘可以自动运行,按照界面中的提示,选择自己感兴趣的题目就可以操作了。

本书有十章,包括了 Microsoft Windows® 2000 Directory Services Infrastructure 考试要求的全部内容,包括 Windows 2000 中的 Active directory 简介、Active directory 的实现及其管理工具、利用 DNS 来支持 Active directory、配置网站、设置和管理用户与组、在 Active directory 上发布资源、管理 Active directory、管理组政策、Active directory 安全和性能管理、远程安装服务。

本书由何学仪策划,武汉理工大学钟珞教授任主编,李辉、夏红霞任副主编。郑巧仙、赵广辉、许再哲、席守卿、孙骏等同志参加了全书的编写工作。

本书是参加 MCSE 考试人员不可多得的一本必备书,也是从事相关技术工作人员的必备工作手册。因为水平有限,书中难免有错漏和不妥之处,望读者指正,以利于改进和提高。

目 录

第一章 Windows 2000 中的 Active Directory 简介

1.1 要点流程

1.2 重点综述

□Windows 2000 纵览

一、Windows 2000 简介

Windows 2000 是多任务操作系统，集成了支持客户机/服务器和对等网络的功能，它结合了能减少所有权总成本的技术，并具有能支持从小型网络到大型企业网络的伸缩性。

一般主要使用 Windows 2000 操作系统的下列两个版本：

①Windows 2000 Professional 该产品是优质、安全的网络客户机和综合企业桌面的操作系统，包含了 Windows 98 的最佳特性，并且大幅扩展了 Microsoft Windows NT Workstation 4.0 的可管理性、可靠性、安全性和性能。Windows 2000 Professional 可单独作为桌面操作系统工作在对等工作组网络环境，或在 Windows 2000 Server 或 Windows NT 域环境下用作工作站。Windows 2000 Professional 还可与 Microsoft Backoffice 产品族共同工作，访问来自 BackOffice 的资源。该产品是适用于各种规模业务的主要 Microsoft 桌面操作系统。

②Windows 2000 Server 该产品是文件、打印、终端和应用程序服务器程序，还可以是 Web 服务器平台，包含 Windows 2000 Professional 的所有特性，加上许多最新的服务器程序专用功能。它对于小型到中型企业应用程序的布置，Web 服务器、工作组和分支办公室是很理想的。

二、Windows 2000 的最新特性

1.第一类基本管理类

①活动目录(Active Directory)：Active Directory 是一种企业类目录服务。该服务是可伸缩的，从头开始直到结束用 Internet 标准技术而创建，全面集成于操作系统级水平。Active Directory 简化了管理，使用户能更容易地找到资源。Windows 2000 的目录服务能力由活动目录来完成。活动目录采用了可扩展的对象存储方式存储了网络上所有对象的信息，并使用这些信息更容易被查找到。活动目录有灵活的目录结构，允许委派对目录安全的管理，提供更有效率的权限管理。此外，活动目录采成域名系统(DNS)，它含有高级程序设计接口。开发人员可使用标准的接口方便地访问和修改活动目录中的信息。

②微软管理控制台(MMC):为了减少新管理员培训时间,提高工作效率,微软提供了一个用于监测网络功能和使用管理工具的统一界面,微软管理控制台的功能接近于人们生活中的"工具箱"。

③组政策(Group Policy):管理员可以通过修改活动目录中的组政策配置客户端的桌面环境,安装应用程序,控制计算机和用户的状态。

④Windows 管理规范(WMI):又称为 CIM for Windows,它提供了统一的访问管理信息的方式。利用 WMI,可以监视、跟踪和控制有关软件应用程序、硬件组件和网络的系统事件,将来自不同来源的数据用通用、标准且逻辑上有组织的方式映像出去,以便在管理数据之间建立相互关系和关联。

2.第二类桌面管理类

①IntelliMirror:管理员可以使用 IntelliMirro 按照用户的特性如职务、组成员身份和位置为用户定义一些策略,用户每次登录网络时,自动地将 Windows 2000 操作系统的桌面重新配置为符合该用户特定需求的系统。而不论其在何处登录。

②Windows 安装程序(Windows Installer):Windows 安装程序是一种允许操作系统管理安装过程的操作系统服务。它管理软件组件的安装、添加和删除,监视文件复原,以及通过复原方式维护基本的灾难性故障恢复。

③远程安装(Remote Install):使用远程安装服务,管理员不用物理访问每一台客户机即可给客户机设置新的操作系统。

④磁盘盘制(Disk Duplication):提供给管理员简单的方法在配置相似的计算机上批量安装 Windows 2000 平台下的操作系统和应用程序。

3.第三类安全类

①安全模板(Security Templates):安全模板是安全配置的物理表示方法,由 Windows 2000 支持的安全属性的文件(.inf)组成。它将所有现有的安全属性组织到一个位置以简化安全性管理。它包含的安全类信息有这样七类:账户策略、本地策略、时间日志、受限组、文件系统、注册表、系统服务。

②Kerberos 验证:Kerberos 验证是 Windows 2000 域中和域间提供验证的主要协议。它提供了更快、更安全的验证和响应,允许用户只登陆一次就可以访问网络资源。

③公钥基础结构(Public Key Infrastructure,PKI):它能够给我们带来强大的安全性,其技术包括智能卡、网际协议的安全机制,加密文件系统。

④二次登陆(Secondary Login):允许用户以普通账户的身份登陆,以另一个用户的身份运行应用程序。在 Windows 2000 中建议管理员以一个普通账户的身份登陆,在执行必要的管理任务时才以管理员的身份运行管理工具。

4.第四类信息发布和共享类

①集成 Web 服务:Microsoft Windows 2000 Server 提供 Internet 信息服务(IIS),该服务可提供在 Internet 或 Intranet 上共享文档和信息的能力。利用 IIS,可以部署灵活可靠、基于 Web 的应用程序,并可将现有的数据和应用程序转移到 Web 上。

②索引服务(Indexing Services):索引服务不仅可以对本地硬盘驱动器及共享网络驱动器上的文档的内容和属性编制索引,还可以控制索引中包括哪些信息。利用索引服务可以使用户轻松、安全地搜索本地或网络上的信息,提高工作效率。

③打印支持:Windows 2000 提供了更灵活的打印支持,包括在 Intranet 或 Internet 上把打

印作业发送到 VRL 地址上，从浏览器中以 HTML 的方式察看打印机和打印作业的信息。此外，当客户端连接到 Windows 2000 打印服务器时，自动下载安装打印机驱动程序。这些新特性大大简化了打印机的配置和使用。

5.第五类应用程序服务类

①消息队列服务(Message Queuing Services)：消息队列是用来确保消息能够到达目标的临时存储位置。消息队列服务确保应用程序可靠的接收和发送信息，支持路由、安全性以及基于优先级的消息传递，使用消息队列，最终用户能够在时断时续的网络和计算机之间通讯，而不必考虑网络和计算机的当前状态如何。

②事务服务(Transaction Services)：事务是一系列工作的集合，事务服务确保事务作为一个整体成功或失败。事务服务允许以部件的方法开发应用，开发人员可以利用部件的灵活性和事务的特性简化开发过程。

6.第六类可扩展性和可用性类

①企业级内存结构(EMA)：Windows 2000 Advanced Server 在 Alpha 平台上支持最多 32G 的物理内存，在 Intel 平台上支持最多 8G 的内存，企业级内存结构允许应用程序使用更多的内存空间，提供更好的性能。

②增强的对称多处理(Symmetric Multiprocessing Process，SMP)：Windows 2000 Advanced Server 支持最多八个处理器，Windows 2000 Datacenter Server 支持最多三十二个处理器。

③群集(Cluster)服务：Windows 2000 Advanced Server 允许把多个服务器连接在一起形成一个系统整体，称之为群集。Windows 群集分为两种：网络负载群集和服务器群集。

④终端服务(Terminal Services)：终端服务提供了客户端远程访问服务器桌面的能力。客户机向服务器送出键盘和鼠标动作。终端服务把该程序的用户界面传给客户机。终端服务提供了远程访问的能力，可以从网络上的任何地方管理服务器。应用程序或用户的数据没有放在客户端，可以提供更好地安全性控制。

7.第七类网络和通信类

①域名服务(DNS)：Windows 2000 中的域名服务支持动态更新(Dynamic Update)、增量区域传送(Incremental Zone Transfer)和服务记录(SRV Record)。动态更新允许 DNS 客户机在发生改动后，自动到 DNS 服务器更新其资料记录。增量区域传送提供在同一区域内传送每个数据库文件版本之间的增量资源记录变化，减少了数据库文件的传输流量。服务记录提供了和 WINS 服务器中存储的 NetBIOS 中第十六个字符相同的功能，用来识别网络资源。

②服务质量(Quality of Service，QoS)：使用 Windows 服务质量，可以控制如何为应用程序分配网络带宽，在应用过程中，可以给重要的应用程序分配较多的带宽，给不太重要的应用程序分配较少的带宽。它为网络上的信息提供了可靠的、端对端快速传送系统。

③资源保留协议(Resource Reservation Protocol，RSVP)：资源保留协议是沿着预先因网络路由选择协议确定的数据路径传送带宽保留的信号传输协议。它允许通讯中的发送方和接收方建立用于保留的 QoS 高速通道，提高联接的可靠性。

④异步传输模式(Asynchronous Transfer Mode，ATM)：ATM 是专门设计用来支持高速通讯的。如果在 Windows 2000 上安装了 ATM 适配器，就可以用附带的 Windows ATM 服务软件来使用 ATM 网络，从而允许网络以最大效率使用带宽资源，并且为有严格的服务要求的用户和程序维持服务质量。

⑤Windows Media 服务：将高质量的流式多媒体传送给 Internet 和 Intranet 上的用户。

8.第八类存储管理类

①远程存储(Remote Storage):远程存储允许使用磁带库来扩充服务器上的磁盘。它使用客户指定的策略自动将不常使用的文件复制到可移动媒体上,在以后需要该文件时,文件的内容又会自动从存储中重新调出来。利用远程存储可把暂时不用的数据存放在相对廉价的介质上,大大降低了数据存储的成本。

②可移动存储(Removable Storage):管理员给应用程序创建媒体池(具有相同管理策略的可移动媒体的逻辑集合)。可移动存储可以很容易地跟踪可移动存储媒体(磁带和光盘),并管理包含这些媒体的硬件库。它使多个程序可以共享相同的存储媒体资源,从而减少开销。

③加密文件系统(EFS):可以在 NTFS 文件系统格式化过的卷上通过对文件或文件夹加密保护文件。使用 EFS 可以防止在未经授权的情况下获取对物理存储的敏感数据访问,以确保文档安全。

④磁盘配额(Disk Quotas):可以在 NTFS 文件系统格式化过的卷上使用磁盘配额来监视和限制每个用户磁盘空间的使用量,也可定义当用户使用的磁盘空间超过指定的阀值时,如何做出响应。

⑤分布式文件系统(Distributed File System,Dfs):管理员可利用分布式文件系统把分布在网络上的资源信息虚拟地放在一个逻辑位置下,这样用户不必到网络上的多个位置去查找他们所需的信息,只需要连接到这个逻辑位置上就可以找到这些资源。分布式文件系统使用户可以更容易地访问文件。

⑥碎片整理(Disk Defragmenter):卷中的碎片越多,计算机的文件系统的 I/O 性能就越差。Windows 2000 中带有碎片整理工具可用于分析文件程度的碎片程序,并可对卷进行处理。

三、Windows 2000 网络环境

基于 Windows 2000 的网络环境,可设置为工作组模型或和域模型。Windows 2000 Professional 和 Windows 2000 Server 可以设置为上述两种模型,这两种产品在管理上的差异,取决于网络环境模型的不同

1.Windows 2000 工作组模型

Windows 2000 工作组是逻辑上的一组联网计算机,它们之间共享资源如文件和打印机。工作组是对等网络,因为工作组内所有计算机能平等地共享资源,而没有专门设置的服务器。工作组内的每台计算机,无论是运行 Windows 2000 Server 还是 Windows 2000 Professional,都有一个本机安全数据库,如图 1.1 所示。本机安全数据库是一个列表,列表记录了用户账号和计算机资源的安全信息。因此,在一个工作组内,用户账号和资源安全信息的管理是分布的。

Windows 2000 工作组具有以下的优点:

·工作组内不需要运行 Windows 2000 Server 以保持集中安全信息的计算机

·工作组容易设计和实施,工作组不需要域所需要的大规模设计和管理

·工作组对于物理上接近,为数不多的计算机来说,是比较方便的

使用 Windows 2000 工作组模式的缺陷为:

·每个用户必须在其想获得访问权的计算机上取得一个用户账户。

·用户账户的任何改变,如更改用户密码或新添用户账号,必须在工作组内的每一台计

算机上进行，如果忘记在其中的某台计算机上新添该用户账号，那么用该用户账号将无法登录到那台计算机，并且无权访问该计算机上的资源。

·设备和文件共享由各台计算机处理，只为在各台计算机上具有账户的用户提供共享。

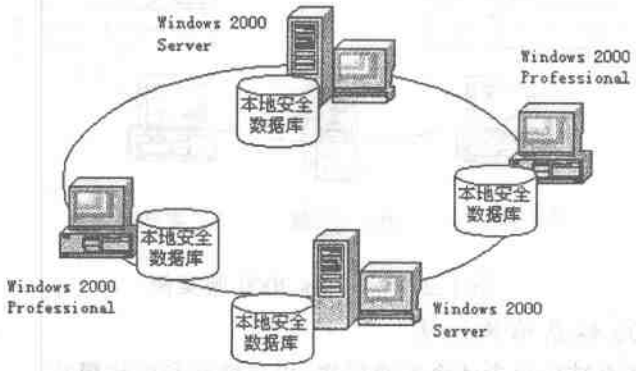

图 1.1 Windows 2000 工作组实例

2.Windows 2000 域模型

Windows 2000 域是逻辑上的一组网络计算机，它们共享一个中央目录数据库，如图 1.2 所示。目录数据库含有该域内用户账户和安全信息，这种目录数据库又称为目录，是 Active Directory 的一部分，而 Active Directory 就是 Windows 2000 目录服务，它取代了以前的所有的“域”(包括多重域)信息存储器。Active Directory 还包含关于服务、其它资源、组织机构甚至更多的信息。

在域内，目录位于被配置为域控制器的计算机上。域控制器是一台服务器，它管理全部的用户域交互作用中与安全有关的问题。其中安全和管理是集中运行的，只有运行 Windows 2000 Server 的计算机，才可以被指定为域控制器。

Windows 2000 域具有如下优点：

·域允许集中管理，因为全部的用户信息都被集中存储。如果某个用户更改了密码，该变化将自动地在域内复制。

·域使用户只需进行单个登录过程，即可访问网络资源，如他们具有权限的文件，打印和应用程序资源。换句话说，只要用户有权访问某些资源，便有权登录某一台计算机，利用网络上另一台计算机上的资源。

·域具有可伸缩性，因此管理员可以创建非常大的网络。

典型的 Windows 2000 域具有以下几种类型的计算机：

运行 Windows 2000 Server 的域控制器。每个域控制器存储并维护目录的一个副本。在域内，只需创建用户账户一次，Windows 2000 Server 将该账户记录在目录中。当用户在域中的某台计算机登录时，域控制器在目录中查找用户名、密码和登录限制，对用户进行身份验证。如果有多台域控制器，则多台控制器之间会周期地复制目录信息。

运行 Windows 2000 Server 的成员服务器。成员服务器是没有被配置为域控制器的服务器，成员服务器不存储目录信息，且不能对域用户进行身份验证。成员服务器提供共享资源，如共享文件夹和打印机。

运行 Windows 2000 Professional 的客户机，客户机运行用户桌面操作系统环境，允许用户访问域内资源。

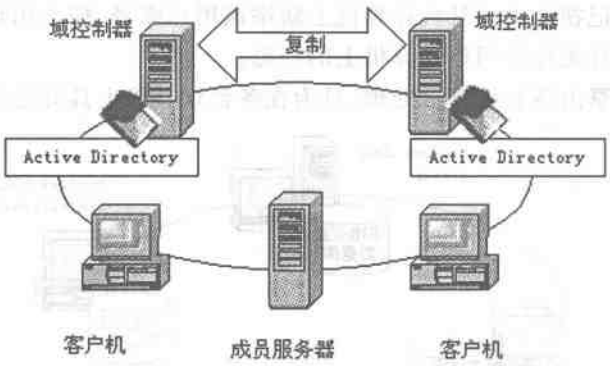

图 1.2 Windows 2000 域实例

四、Windows 2000 体系结构纵览

Windows 2000 体系结构包含两个主要层次:用户模式和内核模式

1.用户模式

Windows 2000 具有不同的用户模式组件:环境子系统和完整子系统。

①环境子系统

Windows 2000 的特性之一,是能运行为不同操作系统而编写的应用程序,Windows 2000 是通过采用环境子系统而实现这种操作的,环境子系统通过为预计可用的应用程序提供应用程序编程接口(API),模仿不同的操作系统。环境子系统接收该应用程序发出的 API 请求,将该 API 请求转化为 Windows 2000 能理解的格式,然后,将转化后的 API 递交执行服务(Executive Sevice)进行处理。

②完整子系统

有许多不同的完整子系统来完成关键的操作系统功能,如安全子系统能跟踪和用户相关的权限和许可权,跟踪被审核的系统资源,接收用户登录请求,初始化登录身份验证;工作站服务和服务器服务构成联网完整子系统,提供 API 访问网络,分别允许运行 Windows 2000 的用户访问网络和提供网络资源。

2.内核模式

内核模式层访问系统数据和硬件。内核模式提供了直接访问内存和在隔离内存区域执行任务的能力。内核模式包含以下四个组件:

①Windows 2000 Executive

该组件执行大部分的 I/O 和对象管理,包括安全任务,但不执行屏幕和键盘 I/O,这些 I/O 由 Microsoft Win32 子系统执行。Windows 2000 Executive 包含 Windows 2000 内

核模式组件,每个组件提供系统服务和内部例程。

②Device Driver(设备驱动程序)

该组件负责将驱动程序调用请求翻译为硬件操作指令

③Micro kernel(微内核)

该组件只管理微处理器。微内核协调所有 I/O 功能,并和 Executive Service 活动同步。

④Hardware Abstraction Layer(HAL,硬件抽象层)

该组件虚拟化或隐藏硬件接口的所有细节,使得 Windows 2000 对于不同的硬件结构更便捷。硬件抽象层含有专门面向硬件的代码,实行 I/O 接口。中断控制器和多处理器通信

机制。

□Active Directory 简介

一、Active Directory 对象和组件

1. Active Directory 对象

①Active Directory 中的对象

Active Directory 存储网络对象的信息。活动目录对象代表网络资源，如用户、组、计算机和打印机。而且，网络中所有的服务器、域和站点都作为对象。因为活动目录代表了所有网络资源(作为分布式数据库中的对象)，只需要一个管理员就可以管理这些资源。

②对象类

对象是一组命名截然不同的属性，每个属性代表一种网络资源。对象属性是目录中对象的特征，例如，用户账户属性可能包括用户的姓名、部门和电子邮件地址。

Active Directory 中，对象按类组织，类是对象的逻辑分组，每个类都是属性的集合

③Active Directory 规划表

Active Directory 规划表定义了可存储在 Active Directory 之中的对象，Active Directory

规划表是一个定义的列表，定义了可存储在 Active Directory 中的对象的种类和信息类型。这些定义本身也作为对象存储。因此，Active Directory 可采用与管理

Active Directory 其它对象一样的对象管理操作，管理规划表对象。

有两种规划表定义：属性和类。属性和类又称为规划表对象或元数据。属性和类单独定义。每种属性只定义一次，且能被用于多个类中。

2. Active Directory 组件

Active Directory 使用组件创建目录结构，满足不同组织的需要，组织的逻辑结构由下列

Active Directory 组件表示：域、组织单元、树和森林。组织的物理结构由网站(物理子网)和域控制器。Active Directory 将物理结构和逻辑结构完全分离开来。

(1)逻辑结构

①域(domain)

域是活动目录中逻辑结构的核心单元，它可以存储数百万个对象。域中存储的对象由管理员设定，共用一个目录数据库。一个域有一个唯一的名字，给哪些由域管理者集中管理的用户账户和组账户提供访问通道。

在 Windows 2000 中，域起着安全边界的作用，保证域的管理者只能在该域中有必要的管理权限，每个域都有自己的安全策略和与其它域的安全联系方式。

域同时也是一个复制单元。在域中，作为域控制器的计算机包含活动目录的副本。在一个特定的域中，所有域控制器都能够得到活动目录中的变化信息，并把这些变化复制给该域中其它控制器。

②组织单元(Organizational Units，OU)

组织单元就是一个可以把对象组织到一个域中的容器，它用来将域内对象组织成逻辑管理组，该管理组镜像实际应用中组织的功能或业务结构。

组织单元可以包含的对象有用户账号、组、计算机、打印机、应用程序、文件共享区和来自同一域的其它组织单元。

域内的组织单元的层次和其它域内组织单元的层次是相互独立的，每个域能够执行各自组织单元的层次。

组织单元提供了一种处理管理任务的方式，它们是能够委派管理授权的最小范围，而且它还提供了一种委托用户和资源管理的方法。

③树

树是单个或多个 Windows 2000 域的分组安排或层安排，可以向现有的父域中添加一个或多个子域创建树，树中的域共享一个连续的名称空间和层次化的命名结构，树具有以下几点特征：

·遵循 DNS 标准，子域的域名是子域附加父域名的相对名称；

·单独一棵树中所有的域共享一个公用规划表，该规划表正式定义了 Active Directory 中的所有对象类型，可以存储在 Active Directory 部署中；

·单独一棵树中所有的域共享一个公用的全局目录，它存储了树中对象的信息

④森林

森林是一个或多个独立的，完全不相关的域树的分组安排或层次上的安排，它具有以下几点特征：

·森林中所有的树共享公用的规划表；

·森林中的树，根据它们的域有不同的命名结构；

·森林中所有的域共享一个公用的全局目录；

·森林中的域独立操作，但森林使整个组织机构内能够通信；

·在域和域树之间存在隐藏的双向传递委托关系。

(2)物理结构

Active Directory 的物理组件是网站和域控制器。可以利用这些组件创建目录结构，即镜像您的组织机构的物理结构。

①网站

网站是单个或多个 IP 子网连接的组合，这些子网通过高度可靠的快速链路连接。通过定义站点，可以为活动目录配置访问和复制拓扑。这样，Windows 2000 就可以使用最有效的链接和时间来安排复制和登录。

创建网站的两个基本原因是为了优化复制通信和使用户能够使用可靠、高速的连接登录到域控制器上。

站点映射网络的物理结构，而域映射组织的逻辑结构。活动目录的逻辑结构和物理结构是彼此独立的，主要有以下几个特点：

·在物理结构和域结构之间没有必然的联系。

·活动目录允许在一个站点可以有几个域，一个域也可以有几个站点。

·在站点和域名空间之间没有必然的联系。

②域控制器

域控制器是运行 Windows 2000 Server 的计算机，存储了域目录(本区数据库)副本。由于一个域可以含有多台域控制器，因此，域内的所有域控制器，都有该目录的域部分的完整副本。

它具有如下几点功能：

·每个域控制器都存储了该域 Active Directory 的全部信息的完整副本，管理这些信息的改变，并可将改变的信息复制到域内其它域控制器。

·域中的域控制器，相互之间复制域内的所有对象。

·域控制器能立即处理一些十分重要的更新，如：使某个用户账户失效。

·Active Directory 还能进行多主控复制。

·在一个域内设置多台域控制器，提供了容错能力。

·域控制器管理用户域内交互作用的各方面内容，如定位 Active Directory 对象和验证用户登录试图。

二、Active Directory 中主要概念

1.全局目录

全局目录是一个信息中央存储库，存储树或森林中的对象信息，如图 1.3 所示。默认情况下，全局目录是由森林中初始域控制器（称为全局目录服务器）自动生成的，它为其主域目录中所有对象属性存储一个完整的副本；为森林中每个域的全部对象属性存储了部分副本，该部分副本存储了搜索操作中用得最频繁的属性。复制到全局目录的对象属性，继承了源域的权限，确保了全局目录中的数据是安全的。

全局目录执行下列主要目录作用：

·初始化登录过程时，它为域控制器提供通用组成员信息，使其能登录网络。

·无论森林中的哪台控制器真正包含该数据，它都能查找目录信息。

当用户登录网络时，全局目录为域控制器提供通用组成员账户信息，便于域控制器处理用户登录信息。

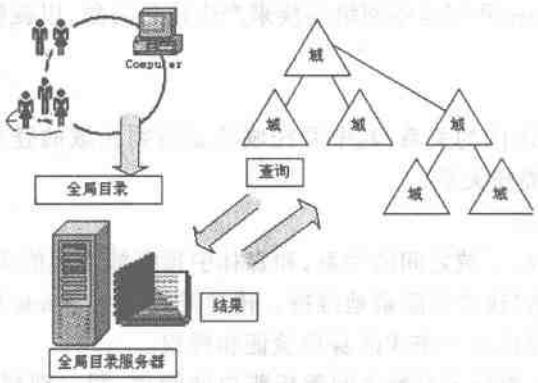

图 1.3 全局目录——中央信息存储库

2.复制

复制确保了某台控制域上的任何改变，都会反映到域内所有其它域控制器上。从而使用户和服务在任何时刻，都能从域树或森林中的任何计算机访问目录信息。目录信息复制到域控制器上，即在网站内进行，也在网站之间进行。

①复制信息的内容

目录中存储的信息被分为三类，每类称为一个目录分区，它是复制的单元。

·规划表信息：它包括目录中能被创建的对象，这些对象可具有的属性，这些信息对域树或森林中所有域都是公用的。

·配置信息：它描述了逻辑结构，包含诸如域结构或复制拓扑结构等信息。这些信息对域或森林中所有域是公用的。

·域数据：描述了域内所有的对象。这些数据是特定域的，不分布到其它域中。

域控制器存储并复制：

·域树或森林的规划表信息；

·域树或森林中所有域的配置信息；

·域本身的所有目录对象和属性，该信息被复制到域内任意附加域控制器中。

全局目录存储并复制：

·森林中规划表信息；

·森林中所有域的配置信息；

·森林中所有目录对象的属性子集(仅在全局目录服务器之间复制)；

·全局目录所在域的所有目录对象和所有对象属性。

②复制方式

·网站内复制

在网站内，Active Directory 自动产生一个拓扑结构，在同一域内的控制器之间使用环结构进行复制。该拓扑结构定义了从一台域控制器到另一台域控制器目录更新的路径，直到所有域控制器都接收到该目录更新。

环结构确保了从一台域控制器到另一台域控制器至少有二条复制路径，如果从网站或网络增加或减少某域控制器，Active Directory 重新配置拓扑结构，以反映该变化。

·网站间复制

为了确保网站间的复制，必须自定义 Active Directory 如何利用网站链路复制信息来表示网络连接。Active Directory 利用这些网络连接来产生连接对象，以提供高效的复制和容错能力。

3.委托关系

委托关系是两个域之间的关系，其中委托域承兑被委托域的登录身份验证。Active Directory 支持两种形式的委托关系：

①隐性双向传递委托

它是一种树内父域或子域之间的关系，和森林中顶级域之间的关系。默认情况下，树内域之间的委托关系(自动)建立并隐蔽地维持。传递委托是 Kerberos 身份验证协议的特征之一，它为 Windows 2000 提供了分布式的身份验证和授权。

域之间的传递委托，消除了对域之间委托账户的管理，同一棵树内的域，立即和树中的每个域建立委托关系，它自动加入到父域的传递、双向委托关系中。结果使得某个域的用户，可访问树域内所有其它被授权的资源。

②显性单向传递委托

它则是不在同一棵树中的域的关系。非传递委托只限定在有委托关系的两个域之间，且不会在森林中其它域传递。大部分情况下，必须显性(手工)创建非传递委托，显性单向传递委托可能存在于：

·Windows 2000 域和 Windows NT 域之间；

·某森林中 Windows 2000 域和另一个森林中的 Windows 2000 域；

·Windows 2000 域和 MIT Kerberos Vs 领域，允许 Kerberos 领域中的客户机针对 Active Directory 域进行身份验证，以访问该域的网络资源。

4.DNS 名称空间

①DNS 名称空间

Active Directory 像其它所有服务一样，主要是名称空间。名称空间是能解析名称的任何

限定区域。名称解析是将名称翻译成该名称表示的某对象或信息的过程，Active Directory 名称空间基于 DNS 命名方案，允许和 Internet 技术互操作，DNS 具有以下优点：

·DNS 名是用户友好的，它比 IP 地址更容易记住；

·DNS 名比 IP 地址更固定。服务器的 IP 地址可以改变，但服务器名保持不变。

·DNS 允许用户使用和 Internet 一样的命名约定连接本地服务器。

②域名称空间

域名称空间是为 DNS 数据库提供层次结构的命名方案，每个节点代表 DNS 数据库的一个分区，这些节点称为域。

DNS 数据库按名索引，因此，每个域必须有个名称。向层次结构加入域时，父域名被添加到其子域。因此，域的名称标识了域在层次结构中的位置。

有二种类型的名称空间：

·连续名称空间　对象层次中子对象包含了父域名。

·不连续名称空间　父对象名和该父对象的子对象名彼此不直接相关。

域名称空间的层次结构，通常包括根域、顶级域、二级域和主机名。

·根域　根域位于层次结构的最上层，用“.”代表。Internet 根域由几个组织机构管理。

·顶级域　顶级域按组织机构类型或地理位置组织，如 gov、com、edu、org、net 等，顶级域可以包含二级域和主机名。

·二级域　一些机构为 Internet 上的个人和组织机构分配和注册二级域。二级域名有两部分：顶级名和唯一的二级名，如 ed.gov 代表美国教育部。

·主机名　主机名指 Internet 或专用网上的特定计算机，主机名是全限定域名（Fully Qualified Domain Name，FQDN）最左边的部分，FQDN 描述了主机在域层次中的确切位置。

5.区

区表示域名称空间的不连续部分。区提供了一种将域名称空间划分为可管理部分的方法。区具有以下几点特征：

·域名称空间的多重区，用来给不同组分布管理任务。

·区必须包含的是连续域名称空间。

·区的名称到 IP 地址的映射，存储在区数据库文件中，每个区都被指定到特定域，即该区的根域，区数据库文件没有必要包含该区根域的所有子域信息，它只包含那些区的子域信息即可。

6.名称服务器

DNS 名称服务器存储区数据库文件，名称服务器可为一个或多个区存储数据。名称服务器有权访问该区包含的域名称空间。

一个区中至少应该有一台名称服务器，对区的改变，如增加域或主机，都是在含有主区数据库文件的服务器上进行，有多台名称服务器充当含有主区数据库文件的名称服务器的备份。采用多台名称服务器具有下列优点：

·执行区传递。区传递是指附加的名称服务器由包含主区数据库文件的名称服务器获取一个区数据库文件的副本。这些名称服务器通过定期查询含有主区数据库文件的名称服务器，以更新区数据。

·提供了冗余性。如果主区数据库文件的名称服务器出现了故障，附加名称服务器将可以提供服务。

·提高了远程访问的速度。如果远程有多台客户机,使用附加名称服务器通过广域网连接线路,可减少查询通信量。

·减少了主区数据库文件的名称服务器负载

7.命名约定

Active Directory 中的每个对象,由名称标识。Active Directory 使用好几种命名约定:可分辨的名称、相对分辨的名称、全局唯一标识符和用户主体名称。

①可分辨的名称

Active Directory 中的每个对象都有一个可分辨的名称(Distinguished Name,DN),它唯一地标识了对象,为客户机从目录中检索该对象提供了足够的信息。可分辨的名称包括:对象所在域名,以及从容器层次结构中到达该对象的完整路径。

②相对可分辨的名称

Active Directory 支持按属性的查询,因此即使不知道确切的可分辨的名称,或可分辨的名称已经改变,也可以定位某个对象。对象的相对可分辨的名称(Relative Distinguished Name,RDN)是对象名的一部分,而对象名是对象本身的一个属性。

可以为 Active Directory 对象复制相对可分辨的名称,但是在同一组织单元内,不能有两个对象具有相同的可分辨的名称。然而,具有相同可分辨的名称的对象,可以存在于不同的组织单元内,因为组织单元本身有不同的可分辨的名称。

③全局唯一标识符

全局唯一标识符(Globally Unique Identifier,GUID)是一个 128 位的数字,以确保它是唯一的。全局唯一标识符在对象被创建时就分配给对象了。它是永远不变的,即使移动对象或给对象更名。应用程序可以存储对象的全局唯一标识符,并利用全局唯一标识符检索该对象,而无论当前可分辨的名称是什么。

全局唯一标识符对于所有的域都是唯一的,这意味着可以在域之间移动对象,而对象的全局唯一标识符不变。

④用户主体名称

它是用户账户的"友好"名。用户主体名称(User Principal Name,UPN)由用户账号的"简写"名和用户账号对象所在树的 DNS 名组成。

三、Windows 2000 网络管理

1.利用活动目录实行集中式管理

活动目录使管理员能够集中管理网络资源。其优点表现为:

·利用活动目录,一个管理员就可以集中管理网络资源;

·利用活动目录,管理员就可以很容易确定对象的信息;

·利用活动目录,可以用相似的管理和安全要求把对象组织到 OU 中。OU 在应用组政策设置和委派管理控制权方面可以提供多层次的管理权利;

·利用活动目录的组政策,管理员可以给站点、域或 OU 指定具体的组政策设置。

2.管理用户环境

利用组政策,可以控制用户数据、个人计算机设置,计算机环境和软件。组政策把活动目录容器(网站、域和 OU)作为管理单元。设置在容器上的组政策可以影响容器内所有的用户和计算机,利用组政策管理用户环境,其主要优点表现为以下几点:

·在用户登录的时候控制用户的使用权限,确定他们所能够和不能访问的内容。