微软指定 MCSE 认证考试试题精解系列丛书

北大宏博

MCSE

Exam 70-217

Windows 2000 目录服务架构

试题精解

中英文对照
包含
交互式全真模拟试题

萧殷　仇伟红　马娟　编著

6-44

北京大学出版社
http://cbs.pku.edu.cn

微软指定MCSE认证考试试题精解系列丛书

MCSE Windows 2000
目录服务架构试题精解

萧 殷 宋梦华 仇伟红 马 娟 编著

北京大学出版社
·北 京·

内 容 简 介

本书是《微软指定 MSCE 认证考试试题精解》系列丛书中的一本。它主要介绍了 MCSE 考试中 Windows 2000 目录服务架构(70-217)部分考查的知识点。全文共包括以下 4 部分内容：考点分析、3 套模拟试题、术语表和考试大纲。文中对考点分析得透彻、独到；模拟试题部分采用中、英文对照进行讲解，便于英文基础薄弱的考生阅读；术语表涵盖了一些常用术语和 MCSE(70-217)考试中的专用术语，便于读者查阅参考；考试大纲为考生复习提供了很好的指导和参考。本书附带配套光盘，提供仿真的模拟考试环境，便于读者进行自我测试。

本书适合于 MCSE(70-217)考生和对 MCSE 知识点感兴趣的读者阅读。

图书在版编目（CIP）数据

MCSE Windows 2000 目录服务架构试题精解/萧殷等编著. —北京：北京大学出版社，2002.1

（微软指定 MCSE 认证考试试题精解系列丛书）

ISBN 7-301-05479-3

Ⅰ.M… Ⅱ.萧… Ⅲ.窗口软件，Windows 2000—工程技术人员—资格考核—解题 Ⅳ.TP316.7-44

中国版本图书馆 CIP 数据核字（2002）第 002440 号

书　　名：MCSE Windows 2000 目录服务架构试题精解

著作责任者：萧　殷　宋梦华　仇伟红　马　娟

责 任 编 辑：赵乐静

标 准 书 号：ISBN 7-301-05479-3/TP・0649

出　版　者：北京大学出版社

地　　址：北京市海淀区中关村北京大学校内　100871

网　　址：http://cbs.pku.edu.cn

电　　话：发行部 62754140　62765127　编辑部 62765126　邮购部 62752015

电 子 信 箱：macrowin@263.net.cn

排　版　者：北京东方人华科技有限公司

印　刷　者：河北省滦县滦兴书刊印刷厂

发　行　者：北京大学出版社

经　销　者：新华书店

787 毫米×1092 毫米　16 开本　23.5 印张　564 千字

2002 年 3 月第 1 版　2002 年 3 月第 1 次印刷

定　　价：42.00 元(含光盘)

前　言

微软认证系统工程师(Microsoft Certified Systems Engineer，简称 MCSE)是微软公司在全世界范围内推出的基于微软产品的网络/系统工程师认证考试。MCSE 认证的难度、力度在国内现有的计算机认证考试中均属上乘，在 IT 领域内得到广泛承认，已经成为 IT 企业以及传统企业的 IT/IS 部门鉴别员工技术水平的重要标准之一。此外，美国、加拿大、澳大利亚、新西兰等国都把 MCSE 认证作为技术移民的能力判断标准之一，获得此项认证者有可能获得免去面试的优待，并可以之代替北美数千所大学的相应学分。

MCSE 考试随着操作系统的版本不断更新，目前和今后相当长时间内将主要是 Windows 2000 版本的 MCSE 考试。该版本的 MCSE 要求应试者通过 7 门考试，包括 4 门核心必考科目(70-210、70-215、70-216、70-217)、1 门核心选考科目(70-219 或 70-220 或 70-221)以及 2 门任意选考科目(任意未过期的考试)。且只要通过上述任意一科考试，即可获得 MCP(Microsoft Certified Professional)证书。MCSE Windows 2000 的常见考试科目如下：

70-210：Installing, Configuring and Administering Microsoft Windows 2000 Professional

70-215：Installing, Configuring and Administering Microsoft Windows 2000 Server

70-216：Implementing and Administering a Microsoft Windows 2000 Network Infrastructure

70-217：Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure

70-219：Designing a Microsoft Windows 2000 Directory Services Infrastructure

70-220：Designing Security for a Microsoft Windows 2000 Network

70-221：Designing a Microsoft Windows 2000 Network Infrastructure

本套丛书是针对 MCSE 考试本身的应试辅导教材，供初步掌握 Windows 2000 操作系统和网络基础知识(学习过微软官方课程或具有相应能力)的应试者在考前 1~2 星期复习知识体系、巩固和检验考试知识点之用。基于上述目的，本书分为考试大纲、知识要点、模拟试题及解析、词汇附录、模拟考试软件等几个部分。其中知识要点部分(第 1 章)以微软公布的官方考试大纲为依据，简要回顾考试中所涉及全部知识点的主要内容，以帮助应试者全面复习巩固。该部分简明扼要但不失全面，从而可以帮助试图快速通过考试的读者以及实践经验丰富但未阅读标准教材的应考者强化复习。本书的主要部分是 3 套模拟试题以及试题解析，模拟试题的形式、长度、难度与实际考试完全相同。全部试题都有相应的中文翻译，以帮助英文基础薄弱的应试者理解题意并提高英文答题能力。本书还对每道模拟试题进行了详细的解析，以供读者更好地理解题意、弄清正确答案的来龙去脉、相关背景知识、引中的知识点内容以及出题者的意图和出题模式，这些分析将有助于应试者在真正的考试中快速、准确地解决问题。鉴于一些读者对 Windows 2000 以及

网络专业的英文术语较为生疏，我们在本书的附录中包含了一个简要的术语表，可供读者快速参考查阅。

本书的配套光盘内包含 3 套交互式的模拟试题，与真实考试形式一致。读者可在完成本书的学习之后用其检验学习效果、或者在考试前进行适应性训练，从而熟悉考试形式、掌握考试技巧。

准备 MCSE 考试是一项系统工程，知识基础、应用能力、应试技巧、英文能力 4 个方面构成了 MCSE 战车的 4 个驱动轮。我们建议的学习方法因人而异，经验不足的应试者在使用本书之前应该学习微软标准 MCSE 课程，以建立系统知识体系，然后以本书作为中、后阶段复习的主要资料以便巩固知识、掌握技巧、提高能力。对于经验丰富、基础扎实的应试者，本书可以作为主要复习资料，提供全面检查漏洞、快速熟悉考试题型、掌握必要技巧的有效工具。

作者

2001 年 8 月

目 录

第1章　知识要点

1.1 安装和配置活动目录

活动目录(Active Directory)是 Windows 2000 的目录服务体系名称，Windows 2000 活动目录包括目录和服务两种类型的实体：目录作为不同种类对象的物理储存容器；服务实现目录中信息和资源的应用。

网络中的用户数据、服务器和打印机都可以看作对象，目录服务的作用就是使管理员能够明确地定义并管理这些对象，以确保用户和应用程序可以方便地利用资源并查询、更新和保护数据信息。Windows 2000 活动目录是一种分布式目录服务体系，它提供可伸缩性、可拓展性、容错性和安全性等多种功能。

活动目录简介

加入活动目录中的任何东西都可以看作对象，对象的层次定义了活动目录的逻辑结构。在活动目录中，对象按照类进行组织，类是对象的逻辑分类方式，例如用户账号、组和 OU(Organizational Unit，组织单元，简称 OU)都可以作为对象类。活动目录包括的逻辑组件如下：

- 对象(Object)：对象是用户创建的对象类的实例，每个对象代表一种真实的网络资源，而对象类只是对象的逻辑分类。
- 属性(Attribute)：属性是对象的特征，给定类型的所有对象具有相同的属性，但它们具有的属性值可能不同。

活动目录使用不同的组件组织对象的目录结构。活动目录组织的逻辑结构包括域、组织单元、树和森林；活动目录组织的物理结构包括站点和域控制器。

活动目录组件逻辑结构

在活动目录中，对资源进行逻辑分组可以简化资源组织工作，这样用户可以使用名称而不是物理位置定位资源。逻辑分组使网络的实际物理结构对用户变得透明。Windows 2000 活动目录的逻辑结构组件按照层次由小到大分别是组织单元、域、树和森林，说明如下。

- 组织单元

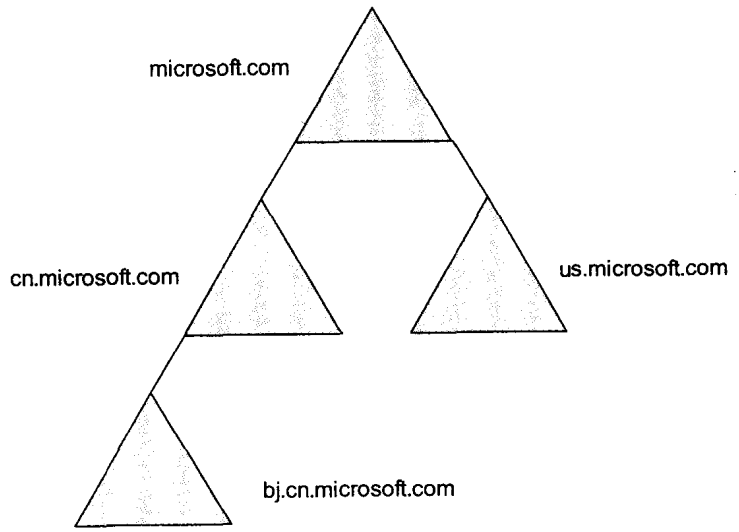
组织单元是一个容器，用于逻辑上组织域中的对象。组织单元中可以包含对象，例如用户账号、计算机、共享文件和应用程序等，组织单元还可以包含本域中的其他组织单元。组织单元可供管理员逻辑上组织域中的用户和资源，使网络管理和公司管理紧密结合。

- 域(Domain)

  活动目录逻辑结构的核心单元是域，它可以跨越物理网络，一个活动目录结构可以包含多个域。域具有如下特征：域可以储存数百万个对象；域负责储存对象的有关信息；域具有独立的安全控制中心，有完整的安全界限，域的 ACL(Access Control List，访问控制列表，简称 ACL)负责储存用户对域中对象的访问权限。域安全信息和 ACL 储存在域控制器上，域管理员具有完全控制域中对象的最高权限。

- 树(Tree)

  树是由 Windows 2000 域组成的逻辑结构，每棵树中包含一个父域，向父域中添加子域即可创建一棵树。树中的域共享一个连续的名称空间和层次化的命名结构。树的特征如下：子域的域名是子域附加在父域域名之后的相对名称。如下图所示，microsoft.com 是父域，即树中的第一个域，附加在该域上的两个子域 cn.microsoft.com 和 us.microsoft.com 继承了 microsoft.com 的域名，其中 cn.microsoft.com 还包含一个子域 bj.cn.microsoft.com，它继承了父域 cn.microsoft.com 的域名。

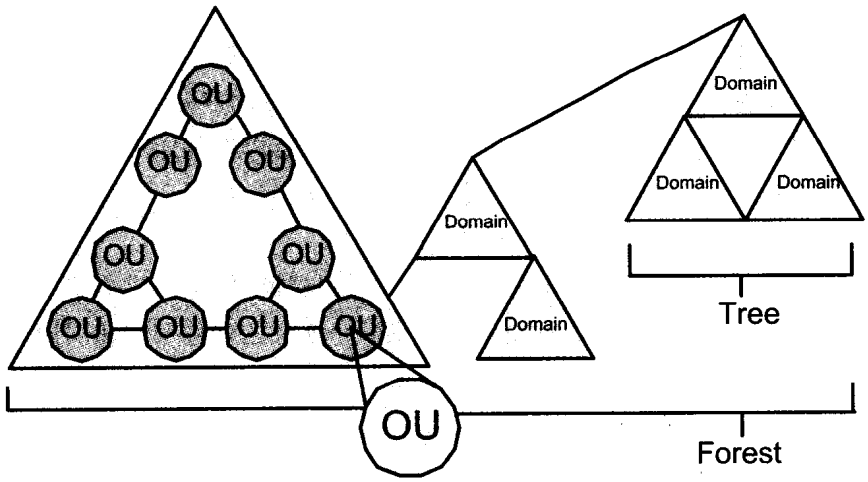


一棵树中所有的域共享一个公共规划表，规划表负责定义活动目录中所有的对象类型。一棵树中所有的域共享一个全局目录，全局目录负责储存树中对象的信息。

- 森林(Forest)

  森林是由若干树组成的逻辑结构。森林具有如下特征：森林中的树共享公共的规划表；森林中的域共享一个全局目录；森林中的域和树之间存在隐蔽的双向委托关系。

下图综合表示了活动目录组件的逻辑结构关系，在 Microsoft 的相应文档和 MCSE 考试的图示题目中，圆型代表组织单元，三角形代表域。



活动目录组件物理结构

活动目录的物理组件包括站点和域控制器，它们反映了实际网络的物理结构。由于活动目录的逻辑组件(主要是域)通常跨越多个物理子网，在资源共享和目录复制管理等方面需要借助于活动目录物理组件规划和配置。活动目录物理组件描述如下。

- 站点

  站点是具有高速局域网(LAN)连接的单个或多个 IP 子网的连接组合，由低速广域网(WAN)连接的各个局域网部分构成一个个站点。每个站点具有明确的 LAN 边界，通常以低速线路将各个站点连接起来。局域网链路通常有以太网、令牌环、ATM 和 FDDI 等 10M/100Mbps 甚至更快的网络；广域网链接通常有电话拨号链接、VPN、DDN 和租用线路等。

- 域控制器

  域控制器是网络中负责储存域数据库副本的 Windows 2000 Server 计算机，一个域中至少有一台域控制器，也可以有多台。域控制器具有如下功能：储存域中活动目录全部信息的副本，并可以将这些信息复制到其他域控制器上；域控制

器负责处理域中对象的更新；域控制器定期将各自做出的改变复制到其他域控制器上；域控制器负责处理用户的登录请求和资源访问请求；多台域控制器提供容错和负载平衡。

活动目录主要概念

Windows 2000 活动目录引入了几个概念，包括全局目录、复制、委托关系和命名约定等，简单介绍如下。

- 全局目录

  全局目录用于储存树和森林中的对象信息，通常树或森林中第一个域的第一台域控制器自动成为全局目录服务器，它负责生成和储存全局目录。全局目录储存主域目录中所有对象属性的完整副本，并储存森林(树)中其他域中全部对象属性的部分副本。这里的部分属性是指日常应用中最频繁使用的属性，它使资源的查询、搜索和定位更加快捷。全局目录的作用是：在初始化登录过程中，为域控制器提供通用组成员账号信息，便于域控制器处理用户登录信息。在本地即可查找到森林(树)中其他域控制器上储存的信息，减少用于跨域查询的网络流量并节省时间。

  虽然默认的全局目录服务器是活动目录中的第一台域控制器，管理员也可以指定其他域控制器作为全局目录服务器。为了提高复制和查询效率、加快响应速度并提供冗余，建议在每个主要站点上都提供一台全局目录服务器。

  通常用户在全局目录不可使用的情况下只能登录本地计算机而不能登录网络，唯一的例外是域管理员(Domain Admins)组成员，他们可以在任何情况下登录网络。

- 复制

  活动目录中的对象信息储存在域控制器上，域控制器也负责对象属性的更新操作，为了确保这些更新能够及时反映到网络中的其他域控制器上，以确保整个活动目录能够及时获知对象属性变化，需要在活动目录域控制器之间配置复制。活动目录中储存的信息类型亦即目录复制中被复制的信息类型如下。

  - 规划表信息：能够在目录中创建的对象以及这些对象可以具有的属性，树和森林共享规划表信息。
  - 配置信息：对象在目录中分布的逻辑结构，包括域结构和复制拓扑结构信息，树和森林共享配置信息。
  - 域数据：描述域中所有对象。

  规划表和配置信息被复制到树和森林中的全部域控制器上，域中的对象信息被

复制到本域的所有域控制器上。每个域的全部对象以及森林中全部对象的属性子集都被复制到全局目录上。

域控制器负责储存并复制以下信息。

- 树或森林的规划表信息。
- 树或森林中所有域的配置信息。
- 本域中所有目录对象及其属性。

全局目录负责储存并复制以下信息。

- 森林规划信息。
- 森林中所有域的配置信息。
- 全局目录所在域的目录对象及其属性。
- 森林中所有目录对象的属性子集。

- 信任关系

  信任关系是活动目录中两个域之间用于账号身份验证传递的逻辑关系，信任关系中的两个角色是信任域和被信任域。其中信任域授予被信任域中的账号登录和访问资源的权限。这样，即使被信任域中的账号和全局组并不属于信任域，它们也能够被授予访问信任域中资源的权限。在 Microsoft 的图示中，信任关系用箭头表示，箭头方向由信任域指向被信任域，双向信任关系用双向箭头表示。活动目录支持两种类型的信任方式。

  - 隐性双向传递信任

    这是同一树中父域和子域之间的关系(有时森林中的顶级域之间也是这种信任关系)，这种信任关系的特点是：隐性，即树中的域之间自动保持这种默认关系；双向，即域之间互相同时保持信任，一个域既是信任域也是被信任域；传递，如果域 A 信任域 B，域 B 信任域 C，那么域 A 信任域 C，信任传递保持这个树中各个域之间的完全信任。

  - 显性单向非传递信任

    这是不同树中的域之间的信任关系，这种信任关系的特点是：显性，只能由管理员手工在域中创建，默认情况下树之间的域不存在任何信任关系；单向，一次只能创建一个单向信任关系；非传递，如果域 A 信任域 B，域 B 信任域 C，并不能说明域 A 信任域 C，非传递保持树之间的信息安全。

活动目录命名与标识

简明目录访问协议 LDAP(Lightweight Directory Access Protocol)是活动目录的主要访问协议，用于引用、定位和检索活动目录信息。活动目录命名规范遵从 LDAP(v2、v3)和 DNS 标准。

在活动目录中，每个对象都有一个 LDAP 名称，LDAP 名称是层次结构化的，对象在活动目录中的位置由 LDAP 完全路径指示。LDAP 名称由以下部分组成：公共名称 CN(Common Name)、组织单元(OU)和域组件 DC(Domain component)。以下是一个 LDAP 名称的例子：

```
CN=Mary,CN=Users,DC=Contoso,DC=COM
```

上例的 LDAP 名称表示：活动目录对象位于一个商业组织中(DC=COM)，该组织有一个叫做 Contoso 的域组件(DC=Contoso)，域组件中包含一个容器称为 Users，活动目录对象是一个叫做 Mary(CN=Mary)的用户。LDAP 名称的各个组成部分是包含的关系，可以把 LDAP 名称分成前后两段，前一段称为后一段的相对 LDAP 路径，例如 CN=Mary，CN=Users 就是该对象在 DC=Contoso，DC=COM 范围内的相对位置。

Windows 2000 提供了用户主体名称以方便记忆，如 contoso.com 中的用户 Mary 拥有用户主体名 mary@consoto.com，其中 consoto.com 是用户 Mary 所在的域目录树。

活动目录的另一种资源定位方式是 DNS。DNS 是域名系统(Domain Name System)的简称，它提供了一整套基于 TCP/IP 网络的资源定位方法。DNS 命名系统是一个称为域名空间的分级树状逻辑结构。各公司和组织也可以使用自己的域名空间创建私有网络名称系统。外部 DNS 名称是唯一的，由 InterNIC(Internet 网络中心)注册。

在活动目录中，用户通过查询 SRV(服务)DNS 资源记录定位活动目录服务。SRV 记录提供主机名或提供请求服务的域控制器 IP 地址。为了在活动目录中找到一个对象，必须进行两个解析过程。

- 服务解析：用户执行 DNS 查询以解析提供活动目录服务(特别是 LDAP 服务)的计算机。
- 活动目录对象解析：在域控制器中执行 LDAP 查询以定位对象在活动目录中的位置。如果被查询的 LDAP 服务器不能提供被请求对象的信息，则它提供被查询对象可能驻留的域名，这一过程称为 LDAP 引用。只要用户初始化一个 LDAP 查询，就可以收到后续的 LDAP 引用查询的结果。

活动目录管理工具

Windows 2000 活动目录的日常管理工作包括管理用户和组、保护网络资源及管理桌面环境等。作为域控制器的 Windows 2000 Server 计算机自动安装活动目录管理工具，它包含在管理员工具组中。常用的活动目录管理工具如下：

- Active Directory Domain and Trust(活动目录域和信任关系控制台)
  用于配置活动目录域之间以及与 Windows NT 4 域之间的信任关系；改变域运行

模式(混合模式或本地模式)；改变域名称系统的配置以及命名规则。

- Active Directory Sites and Services(活动目录站点和服务控制台)
  用于将站点发布到活动目录中，提供网络的物理结构信息，从而提供目录复制等操作的指导性信息。
- Active Directory Users and Computer(活动目录用户和计算机控制台)
  用于创建、删除、修改和整理活动目录中的用户账号、组账号和计算机账号，管理活动目录组件的安全和资源分布。

以上 3 种工具位于管理员工具组提供的活动目录管理控制台(MMC 工具)。管理员工具组中的其他活动目录工具包括：

- Active Directory Schema(活动目录规划表)
  只有在控制面板中添加 Windows 2000 管理工具组件中的 Active Directory Schema 之后，才能使用活动目录规划表管理工具。它用于查看、管理和修改活动目录规划表信息。
- Active Directory Support Tools (活动目录支持工具)
  在 Windows 2000 Server 安装光盘的 Support\Tools 目录下运行 Setup.exe，安装 Windows 2000 活动目录支持工具。典型的活动目录支持工具包括下列命令：Dslutil.exe(检查 DFS 系统运行状况)、Netdom.exe(管理 Windows 2000 域的信任关系)、Pepadmin.exe(监视复制过程以及复制的一致性)、Nlte.exe(提供域控制器列表、信任关系和复制信息)、Movetree.exe(在单一森林的域之间移动活动目录对象)、Dnscmd.exe(检查 DNS 资源记录的动态注册，保护 DNS 更新)、Acldiag.exe(检查用户是否有访问活动目录对象的权限)。

规划活动目录域结构

域是活动目录层次结构的核心组件，规划网络域范围、大小和数量的工作需要依赖于以下信息：网络的逻辑和物理环境、公司的管理需求、用户需求、未来的网络和需求变化。就网络资源的管理方式而言，通常采用以下 3 种方式之一：集中管理适用于规模和业务量较小且网络拓扑相对集中的公司环境；分散管理适用于规模大、分布范围广且业务分散的公司环境；混合型管理方式综合以上两种方式的特点，适用于较为特殊的环境。

域是活动目录的逻辑组织方式，域中包含的对象可以分布于多个物理位置(站点)之间，域中可以包含上百万个对象，通常将需要集中管理的对象规划到同一个域中，共享一套用户账号和资源管理数据库。在决定采用多域规划的时候，应考虑以下问题：分散网络管理、OU 之间的不同安全需求、对象数目庞大、域名系统命名不同、需要分开的管

理。域的上层结构有树和森林，它们之间的区别在于树中的域共享同一个 DNS 域名根，而森林则采用不同的 DNS 命名系统。

规划组织单元

组织单元(OU)是域的下一级活动目录组件，在域中利用 OU 的层次结构可以组织用户和资源，以反映公司的结构。规划 OU 的工作包括设计 OU 策略、确定 OU 层次、委派 OU 模型和 OU 数量等。OU 设计实际上是定义活动目录管理模型，定义系统管理员维护和控制的层次。OU 规划的原则是：浅层次的规划比多层 OU 规划更有优势；OU 应代表那些不受变化的业务结构。

OU 分层的目的是提供具体的管理控制，OU 可以独立地管理，但是在一个已有的 OU 中创建新的子 OU 时，新 OU 将继承原 OU 的属性；通常只有在嵌套式 OU 结构有明显长处时才采用这种模型；OU 不能包含其他域中的对象，为了避免公司结构调整给活动目录结构造成大的变动，应当将 OU 的第一层建立在管理相对稳定的结构上。典型的 OU 规划有以下 3 种方式。

- 基于业务职能的 OU 规划：按照公司的业务职能部门规划 OU，业务部门的从属结构形成 OU 的层次结构，例如二级 OU 代表公司大部门中的子部门。
- 基于地理位置的 OU 规划：位于分散地理位置的公司可以考虑采用基于地理位置的 OU 规划，一级 OU 代表公司的主要地理分布，通常与站点范围重合。
- 基于业务职能和地理位置的 OU 规划：综合上述两种方式的优点，通常一级 OU 代表地理位置分布，二级 OU 代表不同地理位置的职能部门；或者一级 OU 代表公司职能部门，二级 OU 代表该部门在不同地理位置的分布。

规划站点

站点是活动目录物理结构的组成部分，站点的分布只与网络拓扑的物理结构有关，与域及 OU 等活动目录的逻辑结构无关。站点规划主要影响以下两方面的性能：用户账号登录和身份验证时，需要优先查找本站点内的域控制器；站点内的目录复制与站点间的目录复制具有不同的路径和花费，通常站点间复制的频率较低。每个站点中至少拥有一台域控制器以便将身份验证信息本地化。每台域控制器应参与域内或其他域的目录复制工作，复制的流量应不影响网络性能和正常使用。单一局域网往往只要一个站点即可满足需求，具有低速链路连接的网络通常需要指定多个站点。当域控制器不能及时响应用户请求时，应考虑创建具有独立域控制器的分离站点以便规划用户验证流量。

规划域模式

Windows 2000 的域组织结构有两种模式：混合模式(mixed mode)和本机模式(native mode)。混合模式是指从 Windows NT 4.0 向 Windows 2000 网络迁移过程中，PDC(主域控制器)升级到 Windows 2000 Server 之后的域状态；本机模式是完全 Windows 2000 环境下的域模式。Windows NT 4.0 与 Windows 2000 在目录结构、服务器设置和身份认证等方面有许多不同之处，从 Windows NT 4.0 网络升级到 Windows 2000 网络的步骤如下：

(1) 保存一个 Windows NT 4.0 备份域控制器，以备升级失败时能够恢复原有的 Windows NT 4.0 域配置。

(2) 将 Windows NT 4.0 主域控制器(PDC)升级到 Windows 2000 Server，如果 PDC 还没有升级到 Windows 2000 Server，则该域被认为是一个 Windows NT 域，在升级 PDC 和 BDC 的过程中，该域处于中间状态。一旦 PDC 升级到 Windows 2000 Server，则该域成为混合模式(mixed mode)。

(3) 在新的 Windows 2000 Server 计算机上安装活动目录服务，成为新的 Windows 2000 网络中心目录服务器。

(4) 将全部备份域控制器(BDC)升级到 Windows 2000 Server。

安装森林、树和域

在活动目录中实现一个域的步骤是：将一台服务器升级为域控制器、验证服务器升级和连通性、验证活动目录安装、执行其他活动目录组件的安装。

Windows 2000 使用活动目录安装向导执行活动目录安装，安装过程中，一台 Windows 2000 Server 计算机将成为新的活动目录域的域控制器。在命令提示行运行 Dcpromo.exe 命令可以启用活动目录安装向导。在向导升级期间，需要验证 TCP/IP 连通性，验证 DNS 安装和配置，需要提供合法的 DNS 域名，验证 NetBIOS 命名系统的有效性，验证系统管理员身份。管理员也可以预先生成一个文本应答文件，配置 Dcpromo.exe 命令自动在安装过程中指定活动目录参数。升级域控制器之后，新的域已经创建，这时需要检查以下几个方面以验证活动目录安装的有效性：数据库、共享系统卷、默认站点名、全局目录服务器、根域、默认容器及默认域控制器 OU 等。随后，需要利用活动目录安装日志文件和 SRV 资源记录验证活动目录安装。默认情况下，活动目录安装以混合模式创建域，这意味着域中可以包含 Windows 2000 服务器，也可以包含 Windows NT 4.0 服务器，当域中的全部域控制器都升级到 Windows 2000 之后，应将域运行模式转换为本地模式。

创建森林和树的步骤是在使用活动目录安装向导的过程中进行的，管理员可以选择创建新的树、森林或者加入已经存在的树或森林。

创建站点、子网和站点链接

站点等价于一组单个或多个 IP 子网，站点包含最大范围的高速连接网络部分，站点的边界即局域网与低速链路的边界。在站点中的第一台域控制器上安装活动目录时，站点容器中自动创建了一个名为 Default-First-Site-Name 的对象，活动目录安装完成之后，管理员可将 Default-First-Site-Name 更改为站点的名称。后续安装的域控制器将在活动目录中查找与自己 IP 地址位于同一子网中的站点，并自动添加到该站点中；如果没有匹配的站点，则加入域中初始域控制器所在的站点。创建站点的步骤如下：在管理员工具组中启用 Active Directory Sites and Services 控制台 MMC，右击 Site 节点，选择 New Site 命令，在 New Object-Site 对话框中输入站点信息并单击 OK 按钮创建新站点。

TCP/IP 网络中的子网标志着网络中计算机的连接方式。子网信息用于在登录过程中经过身份验证的计算机在同一站点内查找域控制器，还可以用于活动目录复制过程中确定域控制器之间的最佳路径。创建子网的步骤如下：在管理员工具组中启用 Active Directory Sites and Services 控制台 MMC，双击 Site 节点，右击 Subnets 文件夹，单击 New Subnets，在 New Object-Subnets 对话框中指定 IP 地址和子网掩码等信息。成功创建子网之后，可在 Subnets 节点中右击子网节点，选择 Properties 命令打开属性对话框，建立子网与站点之间的关联。

为了在站点之间进行活动目录复制，必须在站点之间创建链接。不恰当的站点链接将导致复制失败，为了保证复制进行，每个站点至少配置一条链接，每个链接可以包含多于两个站点，以便使所有的站点保持良好的连通性。站点中的第一台域控制器安装活动目录时自动创建了一个名为 DefaultIPSiteLink 的对象，这是站点的默认链接，管理员可以更改该链接的名称。活动目录的目录复制可以使用两种网络协议之一：IP 或 SMTP。IP 复制使用远程过程调用(PRC)在站点内部或站点之间进行复制，站点之间的复制按照复制计划进行，IP 复制不需要证书授权；SMTP 复制只用于站点之间的复制，不用于站点内部的复制，SMTP 是异步的，它将忽略调度计划，使用 SMTP 复制必须安装和配置 CA。创建站点链接的步骤如下：在管理员工具组中启用 Active Directory Sites and Services 控制台 MMC，选择 Inter-Site Transports 节点，右击 IP 或 SMTP，选择复制协议并单击 New Site Link，在 New Object-Site Link 对话框中指定站点链接名称以及其他信息，选择该链接连接的两个或多个站点，单击 OK 按钮创建链接。