第 1 章 - Windows 2000 部署规划简介

Microsoft® Windows® 2000 Server Resource Kit Deployment Planning Guide 是设计、规划和开发 Microsoft® Windows® 2000 的工具。阅读此书，您将会在项目管理和功能两个层次上对部署规划的涵义具有透彻理解。本书讲述的规划信息，例如如何管理测试实验室和先导测试项目，将带领您入门。它提供的重要技术研讨也将协助您部署 Windows 2000 技术。

流程规划由本章开始。它包含全书的内容简介，以及 Windows 2000 及其功能的简短概述。然后是案例研究，举例说明四家公司如何开始规划部署流程。最后，本章从 IT 业务的角度出发提供了功能概述。您可以通过此概述开始规划部署流程。

本章内容

开始规划
Windows 2000 系列产品概述
使用 Windows 2000 改进工作方式
Windows 2000 满足业务需求的范例
筹划应用 Windows 2000 功能满足您的业务需求
筹划应用 Windows 2000 功能规划任务列表

本章目标

本章将帮助您撰写下列规划文档：

- 适合您单位的 Windows 2000 产品列表
- 筹划应用 Windows 2000 功能满足您业务需求的计划

Resource Kit (资源工具包)中的相关信息

- 有关开始规划部署流程的详细信息，请参见本书的“ 创建部署路线图 ”一章。
- 有关部署规划详细信息，请参见本书的“ 部署规划 ”一章。

开始规划

要在企业环境中部署诸如 Windows 2000 的新的操作系统，不仅需要得到主管部门的批准和资金，更需要花费心思认真规划。规划开始前，您需要了解 Windows 2000 系列产品。然后了解其功能，并懂得如何利用它们提高单位的生产率和降低总拥有成本 (TCO)。下面两节将概述本章所述的规划流程，以及使用本书的介绍。

有效使用本书

本书可以帮助您设计、规划和实施 Microsoft® Windows® 2000 Professional 和 Microsoft® Windows® 2000 Server 部署。它提供了通过部署 Windows 2000 的主要功能，解决关键业务需求的指南和防止误解的说明。此外，通过无人值守安装工具、脚本和 Microsoft® Systems Management Server 等实用工具自动安装 Windows 2000 Server 和 Windows 2000 Professional 的渐进指导也在本书讨论之列。这些信息按逻辑思路给出，您可以在开始部署时使用。

要实现这些目标，本书包括三类不同的章节：

- 规划章节，其中的信息可帮助您成功开始规划生产应用，如测试和规划等章。

- 技术设计章节，其中的信息可帮助您实施 Windows 2000 的具体功能（如 Active Directory™ 目录服务），并帮助您设计 Windows 2000 网络以满足单位的需要。
- 自动安装章节，提供了通过使用如 Systems Management Server 这样的工具实现 Windows 2000 Server 和 Windows 2000 Professional 自动安装的渐进指导。
- 表 1.1 列出了本书的五个部分以及每部分的章节。

表 1.1 部署规划指南章节

编号	部分/章节标题	类型
	第一部分：规划概述 提供信息帮助您规划部署的方方面面，同时也包含测试和先导测试信息。	
1	Windows 2000 部署规划简介	规划
2	创建部署路线图	规划
3	部署规划	规划
4	建立 Windows 2000 测试实验室	规划
5	实施 Windows 2000 先导测试	规划
	第二部分：网络基础结构的先决条件 提供的信息可帮助您评估目前的网络并规划网络升级。	
6	为 Windows 2000 准备网络基础结构	技术设计
7	确定网络连通性策略	技术设计
8	使用 Systems Management Server 分析网络基础结构	技术设计
	第三部分：Active Directory 基础结构 提供的信息可帮助您规划部署特定的技术功能。	
9	设计 Active Directory 结构	技术设计
10	确定域迁移策略	技术设计
11	规划分布安全性	技术设计
12	规划公钥基础结构	技术设计
	第四部分：Windows 2000 升级与安装 提供关于升级和安装服务器、成员服务器以及终端服务的信息。	
13	服务器自动安装与升级	自动安装
14	使用 Systems Management Server 部署 Windows 2000	自动安装
15	升级和安装成员服务器	自动安装
16	部署终端服务	技术设计
17	确定 Windows 2000 网络安全性策略	技术设计
18	确保应用程序和服务的可用性	技术设计
19	确定 Windows 2000 存储管理策略	技术设计
20	将 Active Directory 与 Exchange Server 目录服务同步	技术设计
	第五部分：Windows Professional/Client 部署 提供的信息可帮助规划和部署 Windows 2000 Professional 客户。	
21	测试应用程序与 Windows 2000 的兼容性	技术设计
22	定义客户连通性策略	技术设计
23	定义客户管理与配置标准	技术设计
24	应用更改与配置管理	技术设计
25	客户安装与升级自动化	自动安装

如何开始规划

规划操作系统的安装与升级需要许多步骤和详尽的计划。本章内容将帮助您开始规划流程。图 1.1 列出了本章所介绍的规划步骤。

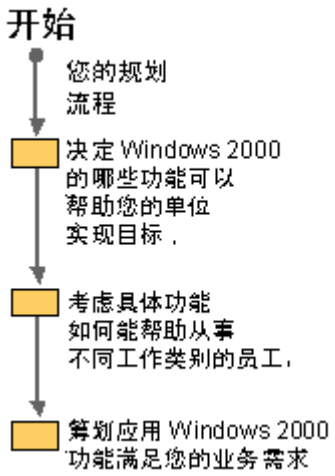


图 1.1 如何开始规划

Windows 2000 产品系列概述

一个组织要在新的数字经济时代保持竞争优势，需要一种先进的基于计算机的客户/服务器基础结构，以降低成本并使组织能够迅速地适应变化。Microsoft Windows 2000 操作平台将 Windows 2000 Professional 和 Windows 2000 Server 结合在一起，可为各种规模的组织带来以下收益：

- 降低了总拥有成本 (TCO)。
- 每周 7 天、每天 24 小时连续计算的可靠的操作平台。
- 可适应迅速变化的数字化基础结构。

整个产品系列的设计可为网络、应用、通讯和 Web 服务提供更高的可管理性、可靠性、可用性、互操作性、可扩展性和安全性。为满足各种规模组织的计算需要，有几种 Windows 2000 产品可供选择。以下各节介绍了构成 Windows 2000 系列的具体产品。

Windows 2000 Professional

Windows 2000 Professional 可使用户在各种工作条件和用户条件（如移动和远程用户）下提高生产率，确保用户数据的最高安全性，并为新一代个人生产力应用程序提供必要的性能。Windows 2000 Professional 通过以下途径帮助您降低总拥有成本：

提高客户管理能力

Windows 2000 允许管理员完全控制客户数据、应用程序和系统设置，使您大大节省致电帮助中心的费用。它还确保用户不会意外损坏系统，并允许用户 24 小时使用完成任务所需的工具，甚至他们在别人的计算机上工作时也能实现这一点。

广泛的管理工具支持 为改善信息技术的可管理性，Windows 2000 Professional 的设计包含了“客户代理”，它使得诸如 Systems Management Server 这样的领先的管理解决方案有效地工作。

使用方便 通过个性化的菜单和“最近使用”列表，用户界面的设计使访问信息变的更加容易。（操作系统确定您使用最频繁的任务，然后将这些任务显示在每个菜单的可视部分。）

更高的稳定性 Windows 2000 Professional 是现有的最可靠的客户和移动操作系统。客户运行时间更长，确保更高的生产率。

更强大的设备支持 Windows 2000 Professional 可支持 7,000 多种设备，包括以前 Microsoft® Windows® NT Workstation 版本 4.0 所不支持的许多设备，如许多早期的打印机、扫描仪和数字相机等。这意味着它所支持的设备种类比 Windows NT 4.0 高出 60%。Windows 2000 Professional 还支持 Microsoft® DirectX® 7.0，这是一组底层应用程序编程接口 (API)，它可以提高基于 Windows 的计算机的媒体性能。

备注 有关所支持设备的详细信息，请参见 Web Resource 页的 Microsoft Windows Hardware Compatibility List（HCL，Microsoft Windows 硬件兼容性列表）链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

配置更加容易 新的向导使得设置和安装 Windows 2000 Professional 时更加容易，无须臆测。

更多语言选项 多语种技术为最终用户和管理员提供了无可比拟的多语种选项。

有关 Windows 2000 Professional 的详细信息，请参见本书第六部分各章。

Windows 2000 Server 系列

Windows 2000 Server 系列包括两种版本：Standard 版和 Advanced 版。Standard 版为基本服务（包括文件、打印、通讯、基础结构和 Web 服务器）提供核心功能，适合于拥有许多工作组和分支机构的小型或中型组织。Advanced 版的设计则旨在为大、中型组织及 Internet 服务提供商 (ISP) 满足关键任务需求，如大型数据仓库、电子商务或 Web 主机服务。

Windows 2000 Server Standard 版

Windows 2000 Server 的核心是一组基于 Active Directory 目录服务的基础结构服务。Active Directory 简化了管理，加强了安全性，扩展了互操作性。它为用户、组、安全服务及网络资源的管理提供了一种集中化的方法。此外，Active Directory 有许多标准接口，允许与多种应用程序和设备的互操作。

Windows 2000 Server 提供了一套全面的 Internet 服务，使组织可以利用最新的 Web 技术。这一集成的、灵活的 Web 平台提供了一系列完善服务，供您部署企业内部网和基于 Web 的商业解决方案。这些服务包括站点托管、高级 Web 应用和数据流媒体。

Windows 2000 Server 扩展了 Microsoft® Windows® NT Server 版本 4.0 所确立的应用服务。Windows 2000 Server 集成了诸如组件服务、事务和消息队列以及可扩充置标语言 (XML) 支持，是独立软件开发商解决方案和自定义业务线应用程序的理想平台。

在过去几年中，随着微处理器快速地更新换代，许多公司都从中获益。为使装有更快处理器的系统增强性能，Windows 2000 Server 还支持单处理机系统和物理内存多达 4 GB 的四路对称多处理 (SMP) 系统。

传统的客户/服务器模式和工作组模式下的客户机和服务器要求具备多任务能力，而运行 Windows 2000 操作系统的商业服务器具备了这一点。您的组织可能还要求对文件和打印服务器、应用程序服务器、Web 服务器和通讯服务器按部门进行部署。在安装和配置扮演这些不同角色的服务器的过程中，本操作系统的一些主要的协助功能包括：

- Active Directory
- IntelliMirror 和组策略
- Kerberos 身份验证和公钥基础结构 (PKI) 安全措施

- 终端服务
- 组件服务
- 增强的 Internet 和 Web 服务
- 多达四路 SMP 支持

Windows 2000 Advanced Server

Windows 2000 Advanced Server 是 Windows NT Server 4.0, Enterprise Edition 的新版本。它提供了一套综合的群集基础结构，使应用程序和服务的可用性和可扩展性大大提高，其中包括在页面地址扩展 (PAE) 系统中支持多达 8 GB 的主内存。 Advanced Server 专为高要求的企业应用程序而设计，使用多达八路对称多处理 (SMP) 支持新的系统。SMP 允许计算机多处理器中的任何一个与系统中的其他处理器同时运行任何操作系统或应用线程。Windows 2000 Advanced Server 非常适合数据库密集型的工作，并且提供高可用性的服务器群集和负载平衡，从而提高系统和应用程序的可用性。

Windows 2000 Advanced Server 包括 Windows 2000 Server 的全部功能，并增加了企业和大型部门解决方案所必须的高可用性和可扩展性。Advanced Server 的主要功能包括：

- Windows 2000 Server 的全部功能
- 网络 (TCP/IP) 负载平衡
- 基于 Windows NT Server 4.0 Enterprise Edition 中 Microsoft Windows Cluster Server (MSCS) 的、增强的、双节点服务器群集
- PAE 系统中主内存多达 8 GB
- 多达八路 SMP

终端服务

Microsoft Windows 2000 Server 的终端服务功能为那些通常无法运行 Windows 的计算机提供了 Windows 2000 Professional 和最新的、基于 Windows 的应用程序。终端服务还提供了远程管理模式，允许管理员对客户进行访问、管理和故障排除。通过终端仿真，终端服务允许相同的应用程序运行在不同类型的计算机硬件上。对于那些希望提高应用程序部署灵活性并控制计算机管理成本的组织，终端服务体系结构大大增强了基于服务器及具有完整功能的个人计算机的传统的两层或三层的客户/服务器体系结构。有关终端服务的详细信息，请参见本书的“ 部署终端服务 ”一章。

使用 Windows 2000 改进工作方式

当您的单位计划迁移到 Windows 2000 时，许多人要问的第一个问题是：“ 它能为我带来什么？ ”您的系统管理员和您的用户都会从迁移到 Windows 2000 中受益。您的管理员将能够提供更强大的移动支持、更容易的客户安装以及更少的管理开销。您单位内的工作人员可以利用更简单的用户界面和增强的可靠性及可用性。不仅如此，个人用户还将感受到为他们从事的特定工作所带来的改进。

让我们看一下 Windows 2000 操作平台如何影响三种不同的工作类别：信息技术 (IT) 主管、部门经理和销售代表，从而帮助您回答 Windows 2000 如何在您的单位内改进工作这一问题。 以下各节并未列出每种工作类别将要使用的全部功能。它们提供的是一个范例，您可用来开始您的规划。

IT 管理员

假设您是一位 IT 管理员，Windows 2000 为您提供了对单位内所有客户的集中控制。管理员还可以使用专为利用 Windows 2000 新技术而编写的应用程序。这些应用程序易于部署、便于管理、更加可靠。结果是，您可以提供更好的服务。下列 Windows 2000 功能是使您工作更有效的 Windows 2000 Server 新技术的实例。

IntelliMirror 和 Active Directory 这些功能允许您运用组策略配置客户，以满足特定用户组的各种不同需求。例如，您可以确保财务部门的每个人都有所需的电子表格、字处理和演示文稿应用程序。同样，您可以把销售跟踪软件指派给销售小组。另外，您可以设置策略，让用户从网络上的任何计算机都能看到他们首选的安排。为降低帮助中心成本，您可以加密保护用户的计算机，不让他们更改计算机配置。

远程安装技术 远程安装（RI）技术允许您使用组策略向客户机上自动安装 Windows 2000 Professional 操作系统。您可以使用这项技术（RIPrep 工具包含在 Windows 2000 Server 操作系统 CD 中）从一个中央位置安装 Windows 2000 Professional 操作系统。您可以将 RI 与 Microsoft® IntelliMirror 技术结合使用以映象一个完整的系统。如果您还使用漫游配置文件，这种功能的结合将在灾难恢复过程中助您一臂之力。

Windows 2000 徽标应用认证程序 Windows 2000 徽标程序是一项 Microsoft 规范，它帮助开发者构建能充分利用 Active Directory、Windows 安装程序和其他 Windows 2000 功能的应用程序，这些功能使得应用程序在公司范围内更加易于管理。利用该规范中的信息，您可以开发使用 Windows 2000 功能的应用程序以降低您的 TCO，还可以开发与您单位目前正在使用的其他应用程序一同良好运行的应用程序。有关 Windows 2000 徽标应用规范的详细信息，请参见 Web Resource 页上的 MSDN 联机链接，地址是：http://windows.microsoft.com/Windows2000/reskit/webresources。

终端服务和移动设备 这些功能允许您从网络上的任何位置管理服务。例如，当您访问一个分公司时接到一个关于网络带宽问题的电话，您可以通过一个无线的掌上型计算机来访问网络的集中管理工具，对该问题进行诊断，将其解决。

部门经理

作为部门经理，您负责协调项目和雇员。由于信息访问途径得到改进，您可以更容易地收集和分析信息。下面的例子说明了 Windows 2000 的一些具体功能如何使您（作为经理）的工作更加容易。

终端服务或更改及配置管理技术 利用更改及配置管理技术，您的管理员可以确保您不论您从哪儿登录到网络，都可以使用所需的软件、数据和桌面设置。如果您正在访问财务组，并且需要查阅一份报表，您可通过终端服务登录到一个瘦客户设备，就象您仍然在自己的办公室里一样。

NetMeeting，服务质量及 USB 即插即用支持 Microsoft® NetMeeting® 允许网络上的多个用户通过视频链路看到对方，并且一同对文档进行实时处理。 为确保视频连接质量不会降低，与 Active Directory 集成的服务质量（QoS）支持允许管理员将更宽的带宽分配给需要的用户和应用程序。此外，通用串行总线（USB）支持允许用户迅速安装即插即用设备，如摄像机。要准备视频会议，您需要做的只是插上摄像机，然后单击通讯簿上适当的名字。

销售代表

使用更改与配置管理技术，您的管理员可确保您总有所需的软件，使您可以方便使用特定的工具和信息。额外功能是为那些将大部分时间花费在主要办公室以外的用户设计的。Windows 2000 的几个功能使您的工作时间效率更高，不论您在路上，还是从办公室主持会议。

同步管理器 同步管理器允许您离线处理信息，就好象您在网络上工作一样。例如，您可以带着客户文件在户外工作，下次登录时将它们与网络上的版本重新同步。同样，您可以从公司的内部网站上下载 Web 页，然后离线处理它们。下次登录时，您可以在您的笔记本计算机上更新内部网信息及存储在网络上的客户记录。

漫游用户配置文件 漫游用户配置文件允许您使用自定义的桌面设置并从网络上的任何位置存取您的文档。旅行时，您可以从任何位置登录到公司网络，存取您的所有数据。您不必再劳神把数据传输到软盘上或通过电子邮件获取关键的信息。

Windows 2000 满足业务需求的范例

组织要从许多不同的角度进行部署，这要看他们计划如何将新的操作系统应用到他们的环境中。大多数组织渐进地（或分阶段地）部署操作系统，以防止停机，并保证关键阶段获得成功。

以下各节提供了一些案例研究和范例，说明了组织如何从产品功能的角度进行部署。这些例子提供了一些企业级组织解决紧迫的商业问题的信息。这些信息有助于您在企业内部推荐和高效使用 Windows 2000。

案例研究 1：北美工业制造商

制造业是该组织的主要业务。产品组装在北美的许多地方完成；然而，他们的营业处遍布世界各地，从而形成了高度分散的全球计算环境。有好几个有多条产品生产线的主要产品部门。分布在世界各地的无数内部小组需要对客户和内部文档进行不同级别的访问。每个部门的用户都需要高水平的基于客户的自定义配置。此外，还有大量的供货商和转包商，他们当中有人需要防火墙内的网络访问，其他人只需要外部访问。网络管理员需要根据每个内部或外部小组的特殊需要提供不同级别的安全措施。

现有 IT 环境

目前，该组织支持混合的 Windows NT Server 4.0 Service Pack (SP) 4 和 UNIX 网络操作系统环境，以及混合的 Microsoft® Windows® 95 (85%)、Windows NT Workstation 4.0 (10%) 和 UNIX (5%) 客户环境。信息技术通过控制分布到较低级别 IT 经理的应用程序和资源集中管理。该组织有很宽的带宽需求，并需要强有力的客户管理。目前，Microsoft® Exchange Server 是用于通讯和进度安排的全球任务关键应用程序。

部署 Windows 2000 的目标

为减少支持开销，该公司希望统一使用一种网络操作系统和一种客户系统。它还将把 Exchange Server 目录服务与 Active Directory 集成到一起，创建公用目录，以加强团队合作。另外，他们还计划扩展为多媒体网络，以利于合作和信息共享。

表 1.2 总结了该公司的 IT 目标并说明了该公司选择 Windows 2000 来实现目标的原因。

Table 1.2 北美工业制造商的 IT 目标

目标	Windows 2000 能够提供：
快速安装配置和节省部署费用，支持和安装一个标准的客户操作系统。	客户管理功能，如 IntelliMirror 及自动客户安装和升级技术，如 Remote Install Services 和 Systems Management Server。
安装一个安全、灵活、强健，可以运行于各种硬件上的网络操作系统。	Kerberos 身份验证和网际协议安全 (IPSec) 等安全功能。提供更多列在 HCL 中的硬件选择。提供即插即用功能。

只部署一个服务器镜像，从而减少部署和管理费用。仅支持一个公用服务器操作平台，并将较小服务器合并成较大的服务器。	负载平衡和额外的处理器支持能力。
维持 Exchange Server 长时间运行，因为这对整个组织十分关键。	Windows 2000 为 Exchange Server 提供了稳定的操作系统平台。
创建集中管理模型，它可以对较低级别的域进行分布控制。	Active Directory 使高级管理员可以将 Active Directory 内的特定单位的控制权下放到个人或组。这就无须多个管理员对整个域进行控制。Active Directory 允许公司模仿其业务模型构建网络环境。
提供与目前 UNIX 服务器之间的互操作能力，并使用共同的安全协议。	域名系统 (DNS) 动态更新协议提供了互操作能力。Kerberos 安全机制在两个操作平台上均能工作。
支持企业之间的其他跨平台安全措施。	分布式安全机制，包括 IPSec、 Kerberos 身份验证和 PKI。
使用一个反映业务需要的网络操作系统和域结构。	Windows 2000 十分灵活，可以克服域和安全性局限，以反映您的业务结构，而无须您围绕服务器操作系统的限制来组织业务。
创建一个大的公司计算机目录。	允许您将 Active Directory 数据与 Exchange Server 合并到一个公共目录中。
扩展为多媒体网络，以利于合作和信息共享。	NetMeeting 允许世界各地的小组相互交谈。QoS 允许您在多媒体网络事件期间分配合适的带宽。即插即用使得为多媒体事件连接摄像机十分容易。

案例研究 2：大型跨国制造商

该跨国组织总部位于欧洲，并在 190 多个国家开设了办事处。由于市场扩大、产品销售增加以及合并和收购，该组织业务迅速增长。该公司生产一系列产品，包括消费及工业电子产品，计算机和仪器。每个单独的生产实体都作为独立的公司在母公司的保护伞下运营。共有 130 多个独立的营业公司，每个公司都有自己的组织结构和财务主管、信息主管和执行官。这将影响组织之间和组织内部的动态结构，因为每个 IT 组织各有其目标、预算、目的和局限。母公司需要对公司间的 IT 合作提供支持和指导。

现有 IT 环境

目前尚没有集中的 IT 业务运营小组，所有营业公司之间几乎没有公用 IT 标准，不论对网络或客户操作系统还是对客户生产力应用程序都是如此。集中的 IT 部门负责跨公司的指导和标准制定。

部署 Windows 2000 的目标

1998 年，该公司的 IT 部门承担了一个设计全球 Windows 2000 Active Directory 体系结构的项目，这是一个跨越每个分散营业公司的统一概念。来自几个营业公司的小组代表专注于 Windows 2000 Server 和 Windows 2000 Professional 的结构和部署，并在必要及适当的时候加以集成。母公司负责开发公用，每个独立的营业公司若有需要便采纳该框架。

表 1.3 总结了该公司的 IT 目标并说明了该组织选择 Windows 2000 来实现目标的原因。

表 1.3 一个大型跨国制造商的 IT 目标

目标	Windows 2000 能够：
建立一个公用 IT 基准，所有营业公司	Active Directory 的森林式结构提供了单

IT 小组都可用它建立自己的全球多运营商模型。	一登录点和全局编录功能。
建立一个公用目录服务，供所有营业公司使用。	Active Directory 十分灵活，易于扩展，可以自定义，以满足各个营业公司的 IT 和业务需要。
建立一个公用模型，用于从 Windows NT 环境迁移到 Windows 2000。	远程安装技术和其他远程或自动安装工具，如 Systems Management Server。
建立一个先导测试应用，作为其他营业公司所有 IT 小组的实施标准。	从其他 Windows NT 域复制一个 Security Principal (安全管理员)的能力以及安全标识符 (SID) 历史记录功能，使安全转移到有回退选项的先导环境成为可能。
建立一个用于所有营业公司的公用客户操作系统。	一个用于桌面型计算机和便携式计算机的公用安全模型。即插即用功能。公用硬件支持。组策略、IntelliMirror 和其他通过 Active Directory 管理的客户管理工具。

案例研究 3：跨国金融服务公司

一个跨国金融服务组织由 7 个独立的营业公司组成，在北美、欧洲、小亚细亚和东南亚设有总部。超过 50 个主要的区域性办事处提供一系列金融服务（投资和个人银行业，资产管理和保险）。每个营业公司都是独立的业务单位；然而，在地区级别上，每个公司可以与一个或多个营业公司共用办公室。

该公司在许多国家的定期严格审查及各个国家财务隐私权、贸易、IT 功能和安全法规制约下运行。因此，需要在网络操作系统和桌面操作系统两个级别上维护安全稳定的系统。

现有 IT 环境

对于所有的营业公司而言没有一个中央 IT 小组，因此整个组织没有全面的 IT 标准。每个公司建立了自己的标准；因而每个公司都有自己的 IT 基础结构。在某些地方，营业公司共用一个网络。在其他地方，网络的数量与共用办公场所的营业公司数相同。尽管区域性办公室通常有域控制器，但是本地办公室，尤其是客户及零售场所维护他们自己的文件和打印服务器。区域性办公室受到自身 IT 功能的局限。

一些金融服务应用程序需要 UNIX 操作系统。目前，所有基础结构服务，例如动态主机配置协议 (DHCP) 和 DNS 都在 UNIX 环境中管理。当公司有能力将运行在 UNIX 服务器上的自定义应用程序迁移到 Windows 2000 时将会用到 Windows 2000 DNS 动态更新协议。

他们目前的网络操作系统环境 95% 运行在 Windows NT Server 4.0 环境下，5% 运行在 Novell NetWare Bindery 下。目前每个公司使用中的客户操作系统包括 80% 的 Windows NT Workstation 4.0；15% 的 Windows NT Workstation 3.51 及大约 5% 的 Windows 95。一些金融服务专家既使用 UNIX 又使用 Windows NT 4.0 客户。

部署 Windows 2000 的目标

其中一个营业公司正在开发自己的 Active Directory 结构，目的是为整个组织创建一个公用全球目录设计。一个由代表各营业公司的 IT 专家小组发起的母公司 IT 先行小组也在开发公司范围内的 Active Directory 结构。

该组织计划安装 Windows 2000 时放弃 NetWare Bindery。在可预见的未来网络中将使用 Windows 2000 和 UNIX 两种操作系统。

表 1.4 总结了该公司的 IT 目标并说明了该公司选择 Windows 2000 来实现目标的原因。

表 1.4 一个跨国金融服务公司的 IT 目标

目标	Windows 2000 能够提供：
有助于标准化，可改善易管理性，提高管理能力并降低 TCO 的跨环境的公用客户操作系统。	改进的硬件支持允许在更大范围内选择公司标准的计算机（桌面计算机和便携型计算机）。改进的电源管理使得在便携型计算机上和桌面计算机上一样易于获取网络信息。可在整个 IT 环境中启用组策略和其他管理工具。
在所有营业公司中，为有不同需求的 IT 环境提供可扩展和可用的公用网络操作系统。	提供群集、负载平衡和处理大量数据存储和复杂对象的能力。单一管理点只需一组管理员。组策略使精细管理所有客户成为可能。
桌面计算机和便携型计算机上的客户安全。	可像保护桌面计算机的安全一样保护便携型计算机的安全。
每个桌面上有多个监视器，可同时跟踪交易并获取客户信息。	允许一个 CPU 支持多个监视器。
提高服务水平的同时，通过减少客户管理降低 TCO。	改进的组策略和与 Systems Management Server 的集成。
减少内部软件开发及相关费用。	组件服务和其他工具，如包含在 Windows 2000 Server 中的 Windows 安装程序，可使创建工具更加容易，并减少花费在开发定制应用程序上的时间。
所有营业公司的公用目录。	Active Directory 足够灵活，可以适应所有的营业公司。
允许每个独立公司拥有自己的子域或域。	Active Directory 设计使用顶级域名作为占位符域，因此允许每个公司拥有自己的子域或域。
在 Exchange Server 和 Windows 2000 Server 之间共用一个目录。	使用 Active Directory 连接器将 Microsoft® Exchange Server 5.5 版目录和 Active Directory 同步。
服务的远程管理。	终端服务以轻型管理模式而非应用程序服务器模式配置。这为管理员进行远程管理提供了又一种选择，不会对服务器性能带来负面影响。

案例研究 4：跨国软件开发公司

有一家开发基于计算机的操作系统以及用户和商用应用软件的知名公司，其总部在美国西部。但其销售、支持和软件开发部门分布在世界各地 180 个地方。该公司的信息技术 (IT) 分部有两个主要职责：

- 提供并维护 IT 系统和解决方案，帮助员工高效率、高效能地工作。
- 与产品开发组合作在企业环境中测试和部署 β 产品。

现有 IT 环境

公司目前的 IT 环境是由纯粹的 Windows NT Server 4.0 和混合了 Windows NT 4.0、Windows 95、和 Microsoft® Windows® 98 的客户构成，同时还包括了许多在用户部门运行 β 软件的计算机。IT 提供集中的：

- 目录服务。
- 邮件和协作服务。
- 管理 Windows NT Server 4.0 的安全服务、网络帐户、Web 服务以及网络。

用户的地理位置遍布全球。80% 到 90% 的员工为他们自己的桌面客户机排除故障。大量的用户要远程访问网络，所以要求有稳定的远程访问服务。IT 还需支持远程办公的人员和需要通过国际接口访问公司网络的员工。

部署 Windows 2000 的目标

该公司的主要目标是在 12 个月之内把所有的服务器和用户升级到 Windows 2000。在迁移时，IT 组必须在维持关键应用程序服务的同时，把资源域折叠到基于不同地点的主控用户域中。去除一些资源域能够减少网络上的服务器数量，简化管理，并且能够减少硬件和软件的支持成本。

IT 部门还必须保证用户属性信息在 Active Directory 目录服务、Exchange Server 5.5 目录服务和公司使用的其他系统间保持同步。所有联机并使用 Active Directory 的系统都必须一同工作。最后，他们想创建公用的控制台目录树和一个公用目录。

表 1.5 总结了该公司的 IT 目标并说明了该公司选择 Windows 2000 来实现目标的理由。

表 1.5 跨国软件开发公司的 IT 目标

目标	Windows 2000 能够提供：
合并全球服务器，加强可管理性，降低支持成本。	Advanced Server 高性能的内存管理和多处理功能使服务器合并成为可能。这些功能增强了平台的可扩展性，使得平台更适合进行服务器合并。
购买最先进的硬件，创建一个新的高速公司网络。	Windows 2000 Server 中的新技术的设计有利于集成计算机结构和微芯片设计的最新成果，包括高级电源管理、USB 设备、 FireWire、智能卡阅读器和红外支持。
根据一种客户进行标准化，以实现更佳的管理控制、颁发机构的委派，以及为远程安装和管理提供更多选择。	通过组策略、由 Active Directory 启用的部门、IntelliMirror 和其他更改和配置管理技术增强了桌面计算机管理。
所有 Advanced Server 的性能和可靠性比 Windows NT 4.0 Server 提高 50%。	核心操作系统在内核级的基线改善增强了内存管理、缓存和优先的多任务处理功能。
由较为复杂的 Windows NT Server 4.0 环境迁移到高度简化的 Windows 2000 环境。	Active Directory 提供了更多的对象存储，更细化的服务器和客户管理，以及通过域名系统和 DNS 动态升级协议使域设计更加简化。
由 Windows NT Server 4.0 域结构变更到有域和目录林的 Active Directory 模型。	Active Directory 提供更灵活的域结构以满足公司当前和未来的需求。
增强公司内部以及与其他公司和用户之间通讯的安全性以及信息共享和事务处理能力。	使用 Windows 2000 Advanced Server 的高级网络和安全设置功能启用一个虚拟专用网络。
增强电子邮件的安全性。	使用 PKI 和证书。
在过渡期间保证公司网络的完全运行。	同时管理和审核运行 Windows NT Server 4.0 和 Windows 2000 Advanced Server 的服务器，包括公司所有的打印机、文件服务器、远程访问服务器、代理服务器和内部 Web 服务器。Windows 95、Windows 98 以及 Windows NT 4.0 客户的互操作性。

筹划应用 Windows 2000 功能满足您的业务需求

在前面几节中，我们已经分别从业务需求、示例公司和用户、产品功能几个高层角度讨论了 Windows 2000 平台的功能和优势。本节将讲述具体的技术功能，以使您能够决定哪种技术对您的单位最重要。在回顾这些功能时，别忘了考虑您单位的短期、中期和长期计划。本书中关于设计的章节将详细讨论每一项技术是如何与其他 Windows 2000 技术集成的，以及设计的依存关系。

下面几节包括了一些 Windows 2000 功能列表，您也许会希望在您单位中部署和配置这些功能。评估所列功能的优势，并决定它们在您单位中的相对优先级别。然后，您就可作出一个及时、合算的部署计划。

本节中所有的表格都可在本书的“计划表示例”中找到。该附录中表格的格式允许输入您对这些功能将在您的单位起到的潜在作用的看法。利用这些工作表做一份自定义摘要，列出您单位需要的 Windows 2000 功能。

备注 以下表格只列出 Windows 2000 Server 和 Windows 2000 Professional 的主要优势，并非所有功能的完整描述。如需某个功能的详细信息，请参阅产品的帮助文件或 *Microsoft® Windows® 2000 Server Resource Kit* 中的相应书籍和章节。

管理基础结构服务

Windows 2000 Server 的管理基础结构服务为 IT 部门提供了实现最高级服务和降低拥有成本的工具。表 1.6 描述了 Windows 2000 Server 的管理基础结构服务及其优势。

表 1.6 管理基础结构服务

功能	描述	优势
目录服务	Microsoft Active Directory 存储网络上所有对象的信息，使这些信息易于寻找。提供灵活的目录层次结构、细化的安全设置委派、高效的权限委派、集成的 DNS、高级编程接口以及可扩展的对象存储。	用一套单一接口即可执行管理任务，如一次登录后就可添加用户、管理打印机和查找资源。开发人员可以更容易地在某个目录中启用他们的应用程序。
管理服务	Microsoft 管理控制台 (MMC) 让管理员用一个公用控制台即可监视网络运行状况，使用管理工具。MMC 是可完全自定义的。	MMC 标准化了管理工具设置，能缩短对新管理员的培训时间，提高他们的生产力。它也简化了远程管理，可以进行委派任务。
组策略	组策略允许管理员定义和控制计算机和用户状态。组策略可在目录服务的任意层次设置，包括站点、域和单位。可根据安全组成员身份筛选组策略。	管理员可利用组策略控制哪些用户可以访问特定的计算机、功能、数据和应用程序。
规范服务	使用 Windows 管理规范 (WMI)，管理员可关联多个来源的数据和事件，这些来源可位于本地或整个组织。	WMI 允许您访问 Windows 2000 对象来创建自定义应用程序和管理单元。
脚本服务	Windows 脚本主机 (WSH) 支持从用户接口或命令行直接执行 Microsoft® Visual Basic	WSH 允许管理员和用户自动化一些操作，如网络的连接和断开。

	Script、Java 和其他脚本。	

有关更多设计和部署 Windows 2000 目录服务和组策略的信息，请参见本书中的“设计 Active Directory 结构”、“规划分布安全性”、“定义客户管理与配置标准”和“应用更改与配置管理”各章。

桌面管理解决方案

桌面管理解决方案的功能可让您更加容易地安装、配置和管理客户，从而降低单位的 TCO。这些功能也被设计为使计算机更易使用的工具。表 1.7 重点列举了 Windows 2000 Server 和 Windows 2000 Professional 能提高用户生产力的桌面管理功能。

表 1.7 桌面管理解决方案

功能	描述	优势
IntelliMirror	IntelliMirror 这一组功能可以使用户在单位内部使用不同计算机时，其数据、应用程序和自定义的操作系统设置会如影跟随。	用户不论是否连接到网络，都可访问自己的信息和应用程序。在应用程序或操作系统升级时，管理员去到每一台桌面计算机的需要大为减少。
Windows 安装服务	控制软件的安装、修改、修复和删除。为打包式安装信息和应用程序的 API 提供模型，与 Windows 安装服务协同使用。	系统管理员可以远程部署和维护应用程序。减少了动态链接库 (DLL) 的冲突数量。启用了自修复应用程序。
远程安装	基于 DHCP 的远程启动技术可以从一个远程地点把操作系统安装到客户的本地硬盘上。网络启动可由以下几种方式进行：预启动运行 (PXE) 环境、启用了 PXE 的网卡、特定的功能键或为没有 PXE 客户提供的远程启动软盘。	管理员不必坐到每一台计算机前安装操作系统。远程 OS 安装也可让您在单位范围内传播和维护一个统一的桌面图像。
漫游用户配置文件	漫游用户配置文件可把注册表值和文档信息复制到网络上的某一位置，这样无论用户在何处登录，用户的设置都是可用的。	用户在旅行时，可随时使用文件和系统信息。
选项组件管理器	Windows 2000 Server 安装程序通过一个安装模块让您可以在安装系统过程中或之后捆绑和安装附件。	减少了部署安装时间，也减少了去到每台计算机的次数。
磁盘复制	您可自定义安装一台 Windows 2000 Server 或 Windows 2000 Professional，然后把它复制到类似的计算机上。	在部署大量的服务器和客户时，复制可以节省时间和金钱。

备注 您可使用 Systems Management Server 来辅助 Windows 2000 的桌面管理技术。

有关更多部署 Windows 2000 Server 和 Windows 2000 Professional 管理方案的信息，请参见本书中的“定义客户管理与配置标准”和“应用更改与配置管理”一章。

安全功能

企业级的安全设置既要灵活，又要有力，这样管理员才能在配置规则、满足安全需求的同时，不会防碍必要信息的自由流动。表 1.8 着重列举了 Windows 2000 的安全功能。

表 1.8 安全功能

功能	描述	优势
安全模板	管理员可以设置不同的全局和本地安全设置，包括安全敏感的注册表值；对文件和注册表的访问控制；系统服务的安全设置。	管理员可以定义安全配置模板，然后通过一次操作就可把这些模板应用到选定的计算机上。
Kerberos 身份验证	Windows 2000 域内部或之间的基本安全协议。支持客户和服务器相互的身份验证，支持通过代理机制进行委派和授权。	降低建立连接时服务器的负荷，从而提高性能。您还可访问其他支持 Kerberos 协议的企业计算平台。
公钥基础结构 (PKI)	可使用集成 PKI 在多种 Windows 2000 Internet 和企业服务包括基于外部网的通讯实现有力的安全机制。	使用 PKI 后，不必创建许多独立的 Windows 2000 帐户，企业就可安全地共享信息。同时支持智能卡和安全电子邮件。
智能卡基础结构	Windows 2000 包括了一个标准模型，用来将智能卡阅读器和智能卡连接到计算机和与设备无关的 API，以启用支持智能卡的应用程序。	Windows 2000 智能卡技术可以用于所有内部网、外部网和公用 Web 站点的安全解决方案。
网际协议安全 (IPSec) 管理	IPSec 支持网络级身份验证、数据完整性和对内部网、外部网和 Internet Web 加密来保证安全。	无须用户交互即可透明实现企业通讯的安全。现有的应用程序可以使用 IPSec 实现安全通讯。
NTFS 文件系统加密	基于公钥的 NTFS 可以针对单个文件或目录启用。	管理员和用户可用随机产生的密钥加密数据。

有关部署 Windows 2000 安全服务的详细信息，请参见本书的“规划分布安全性”和“确定 Windows 2000 网络安全性策略”一章。

信息的发布和共享

Windows 2000 的信息发布和共享技术使得在您单位的内部网、外部网或 Web 上共享信息更加容易。表 1.9 着重列举了信息发布和共享的功能。

表 1.9 信息的发布和共享

功能	描述	优势
集成的 Web 服务	Windows 2000 Server 集成的 Web 服务可让您使用许多 Web 发布协议。	更加灵活地在外部网、内部网或 Web 上发布信息。
索引服务	集成的索引服务可让用户在不同格式和文件中进行全文搜索。	提高生产力。
可移动存储	包括服务器和工具组件，可通过网络提供音频、视频、图示音频和其他多媒体形式。	为培训、协作和共享信息提供了新的机会。提高生产力。
打印	Windows 2000 把域内所有可用的共享打印机放在 Active Directory 中。	用户可以迅速地找到最方便的打印来源。

有关更多部署 Windows 2000 信息的发布和共享服务信息，请参见本书中的“升级和安装成员服务器”一章和 *Microsoft® Windows® 2000 Server Resource Kit Internet Information Services Resource Guide*。

组件应用服务

作为一个开发平台，Windows 2000 支持组件对象模型 (COM) 和分布式 COM (DCOM)，这样开发人员能够更高效地创建更多可扩展的基于组件的应用程序。表 1.10 着重列举了组件应用服务的功能。

表 1.10 组件应用服务

功能	描述	优势
队列组件	开发人员和管理员可在部署时选择合适的通讯协议（DCOM 或异步）。	开发人员无须编写任何代码即可很容易地利用由 Windows 2000 Server 中集成的消息队列服务所提供的存储和转发服务。
发行和预订	COM 事件为所有 Windows 2000 Server 应用程序提供了统一的发行和预订机制。	开发人员不必重建基本服务或对其再次编程。
事务服务	通过调用大型机上的应用程序或从消息队列发送或接收消息提供信息更新。	为开发人员提供了在更新多个数据来源时保证应用程序正确的方法。
消息队列服务	保证消息事务或者完成或被安全地退回到企业环境。	开发人员可以创建和部署能在不稳定的网络上可靠运行的应用程序，并可与不同平台上运行的应用程序协同工作。
Web 应用服务	开发人员可用 Active Server Pages 在当前基于服务器的应用程序上建立基于 Web 的前端。	Web 应用服务允许通过 Web 浏览器以最低的连接成本管理远程服务器。

有关部署 Windows 2000 Component Application Services （Windows 2000 组件应用服务）和 Microsoft® Security Support Provider Interface（Microsoft 安全支持提供商接口）的详细信息，请参见本书的“确定 Windows 2000 网络安全性策略”一章。有关供开发人员使用的详细信息，参见 Web Resource 页的 MSDN Platform SDK 链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

备注 您可与应用程序开发组人员讨论这些功能及其潜在的商业价值。他们的专业知识会有助于您判定这些技术对您单位的潜在商业价值。

可扩展性和可用性

速度更快的 CPU 和网卡是网络性能的传统指标。在将来，更高效的读/写能力、更佳的输入/输出 (I/O) 性能以及迅速的磁盘访问将会成为网络结构中同等重要的因素。需要关键任务计算机的环境现在可以使用 Windows 2000 的扩展功能。表 1.11 着重列举了 Windows 2000 中协助您提高网络可扩展性和可用性的功能。

表 1.11 可扩展性和可用性

功能	描述	优势
企业内存结构	Windows 2000 Advanced Server 允许访问处理器上高达 32 GB 的内存。	允许对大数据集执行事务处理或决策支持的应用程序在内存中保留更多数据，从而提高性能。
增强的对称多重处理 (SMP) 可扩展能力	Windows 2000 Advanced Server 已优化为八路 SMP 服务器。	单位能够充分利用更快的处理器。
群集服务	两个或更多的服务器可以作为单一系统一起工作。	使用简化的管理，即可增加可用性、可靠性、稳定性和安全性。

智能输入/输出（I2O）支持	I2O 使主机的主要 CPU 不必再处理中断频繁的 I/O 任务。	提高了高带宽应用程序的性能。
终端服务	通过终端仿真，终端服务允许相同的应用程序运行在不同类型的客户硬件上，包括瘦客户机、早期的计算机或不运行 Windows 的客户。也可作为一个远程管理选项。	可集中管理任务型工作人员的应用程序和桌面计算机。提供了把当前的桌面计算机桥接到纯粹 Microsoft® Win32® 环境的技术。远程用户用拨号远程访问连接即可得到如本地网络般的性能。可对 Windows 2000 Server 进行图形化远程管理。
网络负载平衡	可以把多达 32 台运行 Windows 2000 Advanced Server 的服务器组合成一个负载平衡的群集。常被用来在其群集的 Internet 服务器应用程序间分发传入的 Web 请求。	通过组合两个或更多主机（是群集成员的服务器）的功能，提高 Web 服务器、文件传输协议（FTP）服务器、数据流媒体服务器和其他关键任务程序的可用性和可扩展性。
IntelliMirror	IntelliMirror 让用户不连接到网络时，也可使用自己的数据、应用程序和设置。	不论用户是否连接到网络，其数据永远唾手可得，眼中的计算环境也是永远一致的。

有关部署 Windows 2000 群集服务的详细信息，请参见本书的“确保应用程序和服务的可用性”一章。

有关终端服务的详细信息，请参见本书的“部署终端服务”一章。

网络和通讯

要想改善您的网络环境，请考虑表 1.12 中所列的 Windows 2000 技术，这些技术能给您更多的带宽控制、安全的远程网络访问和对新一代通讯方案的本机支持。

表 1.12 网络和通讯

功能	描述	优势
DNS 动态升级协议	不必再手动编辑和复制 DNS 数据库。	减少支持网络所需的 DNS 服务器数量，降低管理和设备成本。
服务质量(QoS)	QoS 协议和服务为 IP 通信提供了一个有保障、端到端的快速传递系统。	允许您设定网络通信的优先级，保证能够完成关键处理，数据能够快速和准确地到达。
资源保留协议（RSVP）	该信号传输协议允许发件人和收件人建立一条保留路径，按指定的服务质量进行数据传输。	提高连接的可靠性，加速数据的传输。
异步传输模式（ATM）	ATM 网络可以同时传输大量的网络通信，包括声音、数据、图像和视频。	在单一网络上统一多种类型的通信可以显著地降低成本。
数据流媒体服务	在网络上传递多媒体文件的服务器和工具组件。	数据流媒体通过提供联机会议和信息共享，显著地降低了旅行、团队协作和培训成本。

光纤信道	通过在连接中映射公用的传输协议并合并网络和高速输入输出，光纤信道提供 1 Gbps 的传输速度。	与小型计算机系统接口 (SCSI) 技术比较，提高一些高开销应用程序的灵活性、扩展性、管理性、容量和可用性。
IP 电话服务	电话服务 API 3.0 (TAPI) 综合了 IP 和传统的电话服务。	开发人员可以象在传统电话网络上所做的那样，用 TAPI 创建能在 Internet 或内部网上工作的应用程序。

有关 Windows 2000 网络和通讯功能的详细信息，请参见本书中的“为 Windows 2000 准备网络基础结构”和“确定网络连通性策略”一章。

存储管理

Windows 2000 Server 提供的存储服务既能提高可靠性，又能改善用户访问。表 1.13 列举了这些服务。

表 1.13 存储管理

功能	描述	优势
远程存储	监视本地硬盘上的可用空间数量。当主硬盘上的可用空间降到可靠运行所需的水平之下时，远程存储会清除已复制到远程存储器的本地数据。	管理员可以把文件迁移到从用户角度看还是可用的磁带库中，以此来管理可用磁盘空间。
可移动存储	管理员可以管理可移动存储设备和功能。管理员可以创建由一个特定应用程序拥有和使用的媒体池。	管理员可以通过控制数据的存储位置来优化网络性能。多个应用程序可以共享同一存储媒体资源。
NTFS 文件系统增强	支持性能增强功能，如文件加密、无须重新启动即可在 NTFS 卷中添加磁盘空间、分布式链接跟踪以及通过每个用户卷配额来监视和限制磁盘空间使用。	文件加密可以降低无授权用户看到保密数据的风险。能够迅速地增加分区可以减少网络故障时间以及降低数据丢失的风险。
磁盘配额	有助于管理员规划和实施磁盘的使用。	减少硬件管理的需要，降低维护成本。
备份	用户可以把数据备份到不同的存储媒体，包括硬盘驱动器、磁性和光媒体。	帮助防止因硬件或存储媒体故障导致的意外数据丢失。
分布式文件系统 (Dfs) 支持	管理员可以创建一个目录树，包括多个文件服务器和文件共享目录，Windows 2000 客户可以和任何有匹配协议的文件服务器实现互操作。	Dfs 使管理员和用户更容易找到和管理网络上的数据。Dfs 还提供了容错共享区，可存放重要的网络文件。

有关部署 Windows 2000 Server 存储管理的详细信息，请参见本书的“确定 Windows 2000 存储管理策略”一章。

筹划应用 Windows 2000 功能规划任务列表

当开始 Windows 2000 部署规划流程时，请运用表 1.14 中的规划任务列表。

表 1.14 筹划应用 Windows 2000 功能规划任务列表

任务	章节中的位置
了解本书的结构将有助于您的部署规划流程。	开始规划
了解 Windows 2000 产品系列。	Windows 2000 系列产品概述
分析如何利用具体的功能提高工作人员的生产力。	使用 Windows 2000 改进工作方式
根据您的业务目标审视 Windows 2000 的功能。	筹划应用 Windows 2000 功能规划任务列表

第 2 章 – 创建部署路线图

要合理有序地实现 Microsoft® Windows® 2000，部署规划项目是重要的一步。由于 Windows 2000 可以根据不同规模组织的业务需求和信息技术（IT）能力以增量的方式进行部署，因而需要确定哪些功能适合于您所在的组织。除此之外，还需要考虑您所选择部署的 Windows 2000 功能的技术和项目管理依存关系。最后，需要考虑当前 IT 环境的互操作性或共存需求。

本章将向您描述全面的项目管理过程并指明关键的部署阶段，以帮助您创建一个项目规划（或者称为路线图），使您的小组在单位部署 Windows 2000 时可以有所依照。

本章内容

创建项目规划
部署方案
技术依存关系
规划 Windows 2000 部署的窍门
规划任务列表

本章目标

本章将帮助您完成下列规划文档：

- 项目规划。
- 适合于您所在单位的项目管理过程。

Resource Kit（资源工具包）中的相关信息

- 有关如何制定部署项目规划的详细信息，请参见本书的“ 部署规划 ”一章。
- 有关如何成功地运行 Microsoft Windows 2000 先导测试项目的详细信息，请参见本书的“ 实施 Windows 2000 先导测试 ”一章。
- 有关设计测试实验室和评估 Windows 2000 功能的详细信息，请参见本书的“ 在实验室环境中测试 Windows 2000 ”一章。

创建项目规划

为部署 Windows 2000 创建一个项目规划可以确保成功地进行部署。尽管您会制订一个专门针对您的业务和 IT 需求的项目规划，但在规划中还需要包括一些共同的要素，使之成为项目的一份行之有效的路线图。本章将集中讨论如何将初步的技术决策集成到项目管理规划中，以便用于部署 Windows 2000。有关制定项目规划时需要考虑的具体项目管理事项的详细信息，请参见本书的“ 部署规划 ”一章。图 2.1 显示了创建项目规划的一些步骤。

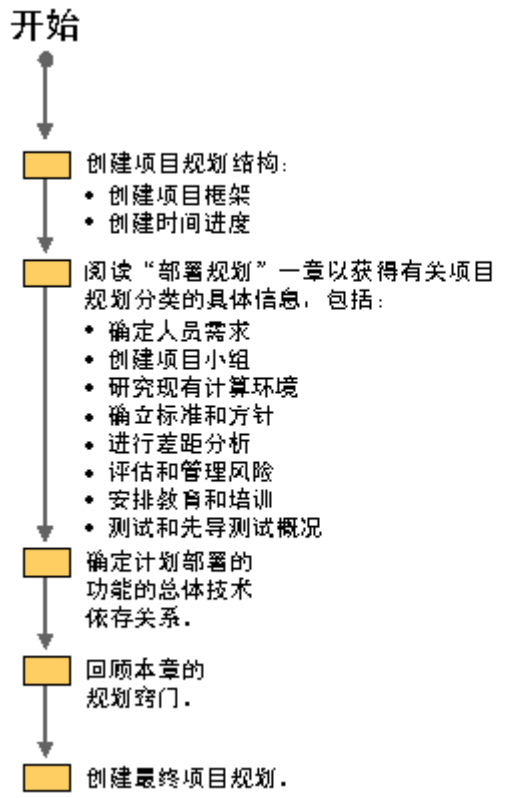


图 2.1 创建项目规划

如果有效地利用项目规划，它能够清楚地确定部署过程中的具体阶段并提供一个清晰、实用的路线图。当然，您不必象遵循安装步骤一样恪守部署过程，基础结构部署过程为 Windows 2000 部署项目提供了一个概念性的框架，同时方便您的部署小组对进度进行评估。

许多单位都已形成了自己的项目管理方法和结构。为使部署取得最大的成功，请依照适合于您单位的项目管理结构。以下各节将概述一个项目管理结构的示例并描述两个示例公司所使用的项目管理结构。

读完本章后，您就会找到有关部署小组、项目规划文档、创建和使用测试实验室以及对 Windows 2000 进行先导测试的参考信息。表 2.1 列出了本书的其它各章，它们包含了更多帮助您制定项目规划的信息。

表 2.1 本书包含的部署规划信息

章节	描述
部署规划	包含了分析当前计算环境、差距分析、人员需求、规划任务、规划部署文档、容量规划、风险评估、教育和培训方面的信息。
建立 Windows 2000 测试实验室	包含有关设计、构建和管理测试实验室；为部署进行测试；部署后测试的信息。
实施 Windows 2000 先导测试	包含有关如何成功地运行 Windows 2000 先导测试项目的信息。
测试应用程序与 Windows 2000 的兼容性	包含有关测试应用程序（包括自定义应用程序和零售应用程序）与 Windows 2000 配置的兼容性的信息。

制定项目规划流程

每个部署项目都经历一个生命周期，从确定 IT 目标、功能设计和开发、执行先导测试项目，直到将这个新的操作系统安装到您的生产环境中。一个项目规划流程的主要功能是为您的部署小组指定、实施、测试和执行必需的活动建立一个顺序。

图 2.2 显示了一个部署 Windows 2000 的项目管理流程的示例。图的顶端列出了其中的各个阶段。图的主体部分包含了在部署的不同阶段需要完成的任务，并给出了您可能考虑的 Windows 2000 的技术建议。

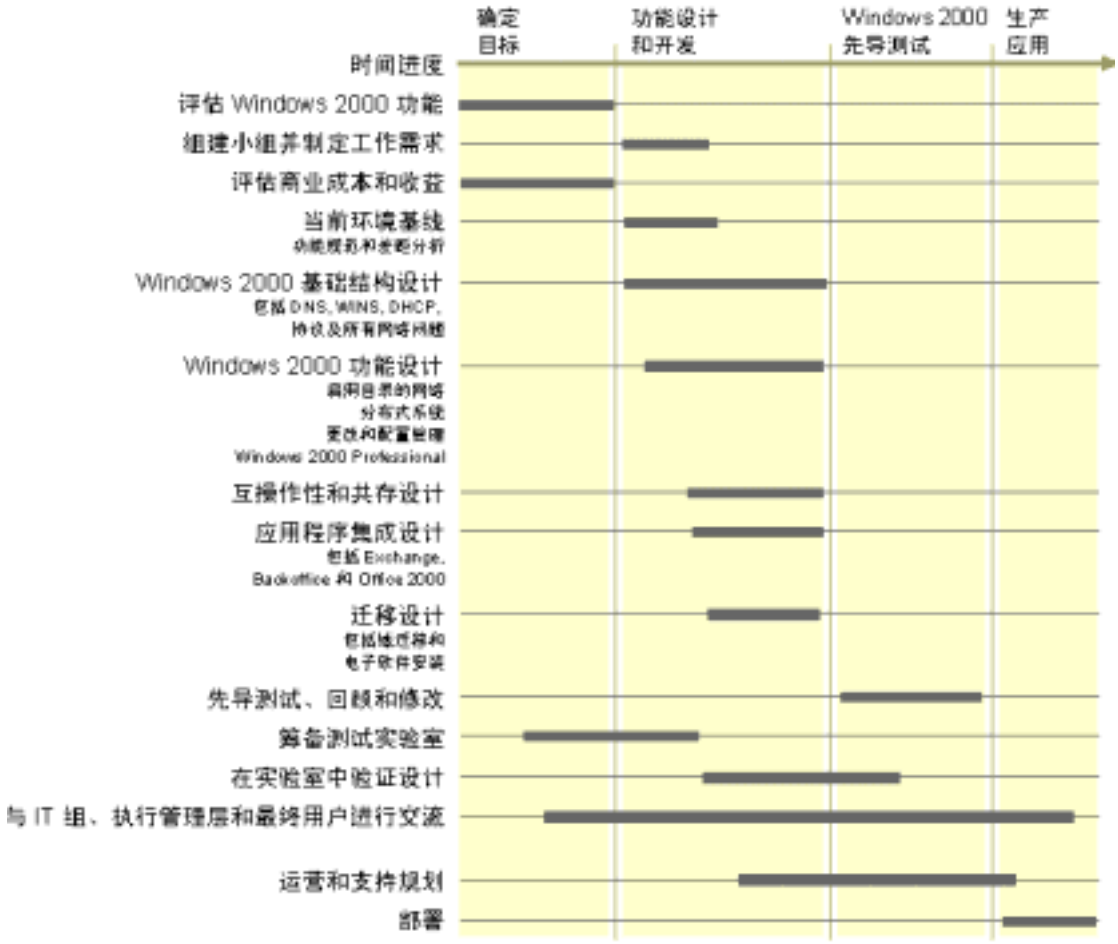


图 2.2 Windows 2000 项目管理流程示例

图中靠近底部的两个进度条指测试实验室。测试是 Windows 2000 部署中不可分割的一部分，在整个部署流程中都要用到。

图 2.2 中所显示的四个项目管理步骤在以下各节中将一一阐述。

确定目标

在这个阶段中，要对与您单位需求相关的 Windows 2000 功能进行评估。同时，您需要获得主管部门的资助和资金、确立目标，并成立一个部署小组。最后，开始使用测试实验室来探索 Windows 2000 的功能。

第一个阶段点是上级部门批准了在您的单位部署 Windows 2000 的整体规划。制定规划时，首先勾勒出部署的高层次的业务和 IT 目标，为实施指明一个清晰的方向。同时，要清楚地确定部署的不同阶段中要包括的 Windows 2000 的功能。

这个阶段要回答的一些问题包括：

- 您的组织为何要部署 Windows 2000？
- 您的组织将从 Windows 2000 中获得哪些商业收益？
- 您的组织将从 Windows 2000 中获得哪些 IT 收益？
- 您的组织目前的 IT 环境与您所希望的环境有何不同？
- 本项目需要何时完成，何时是最后期限？
- 本项目的范围内内容和范围外内容是什么？
- 本项目影响到哪些用户？
- 影响成败的关键因素有哪些？
- 有哪些风险？
- 此流程要涉及哪些集团、组织和个人？

为此阶段点创建的一些文档可能要包括：

- 目标文档。
- 当前环境概况，包括用户配置文件。
- 风险评估。
- 差距分析。

有关风险评估和差距分析的详细信息，请参见本书的“部署规划”一章。

这个阶段对于创建部署路线图十分重要。在明确了目标之后，确定所需要的 Windows 2000 功能以及这些功能如何与您现有的环境相适应就比较容易了。您的分析还可以帮助您理解重要的技术依存关系。尽管需要进行彻底的评估，但这一阶段在短时间内便可以完成。目标阶段帮助您明确一个由 IT 部门、最终用户和管理层共同参与的项目前景，并能帮助您成功地进行部署。

备注 您的单位可能已经正式或非正式地完成了这一阶段。如果管理层已经作出了部署 Windows 2000 的决定，在功能设计和开发阶段开始之前，您依然需要创建一个目标报告并获得正式批准。

功能设计与开发

在功能设计和开发阶段中，将为在您单位中实施的 Windows 2000 功能创建实际的设计（有时称为功能规范）。此时还需确定所选的功能在生产环境中将如何发挥作用。

在这个阶段中，Windows 2000 功能的技术依存关系尤为重要，因此，不同的部署小组需要互相协作，沟通对每种功能的能力、功能和依存关系的理解。本书后面的技术设计各章将帮助您确定如何在您的单位中部署具体的功能。

功能设计规范是一套完整的设计，需要进行测试和改善。例如，根据不同的业务或 IT 需求，您的 Microsoft® Active Directory™ 名称空间可能会有多种不同的设计，每种设计都将根据是否适合于您单位的业务和 IT 标准进行评估。最后，通过技术测试和分析，您将可以为您单位开始实施一个 Active Directory 名称空间。请记住，这一流程及其结果是专门针对您的单位的。

随着各个部署小组创建了自己的规划，通过相互协调达到同步，进而创建一个综合的设计规范，这个阶段的反复设计和测试过程就开始了。在这一阶段，由于需要对各种配置进行测试以确定如何让 Windows 2000 的功能来达到项目目标，因此测试实验室同样也很重要。

功能设计规范需要为项目小组提供关于您单位要部署的功能与特性的足够多的细节，以便于他们确定实施 Windows 2000 基础结构的资源需求和投入。

在这一阶段，还要创建一个项目规划，包含功能规范（各个小组规划的汇总）和进度表。在管理层批准可以进行部署之后，就可以开始实施您的项目规划了。可以包括在规划中的一些主要文件有：

- 功能设计规范
- 更新的风险管理规划
- 主控项目规划和主控项目进度表
- 功能规划，列出哪些功能是范围之内的，哪些是范围之外的

Windows 2000 先导测试

完成了功能设计与开发、并对功能配置进行了彻底测试之后，就可以开始进行先导测试项目了。部署小组需要确定一系列临时性的交付阶段点，每个阶段点涉及解决方案开发、测试、依照预先指定的性能标准进行验证，以及重新设计。跟踪并迅速地解决部署中出现的问题对能够按时按预算达到预期的部署目标至关重要。

在先导测试项目开始运行并趋于稳定之后，主管部门和部署小组就可以共同评估新的 Windows 2000 基础结构的功能并验证生产应用和支持规划已经到位。在这一阶段，主要阶段点和部署文档可以包括：

- 完成技术验证
- 完整、稳定的功能规范
- 完成概念论证
- 完成生产测试
- 完成先导测试
- 更新的风险管理计划

其它您可能希望制定的部署文档包括：

- 培训计划
- 支持或帮助中心计划
- 经营转移计划
- 灾难恢复计划
- 工具列表

在这一阶段，您将根据先导测试对设计进行调整。由于要将部署的每种功能的设计集成在一起，然后测试这些设计以确保集成恰当，您会发现需要进行一些更改。

有关在概念论证实验室测试和先导测试过程中验证和测试 Windows 2000 Server 部署规划的详细信息，请参见本书的“建立 Windows 2000 测试实验室”和“实施 Windows 2000 先导测试”一章。

有关测试应用程序与 Windows 2000 Professional 兼容性的详细信息，请参见本书的“测试应用程序与 Windows 2000 的兼容性”一章。

生产应用

Windows 2000 项目的最后阶段是生产应用。到目前为止，已经在实验室中测试了所有的设计并进行了先导测试以改善规划并进一步测试设计。现在，就可以开始在企业中逐步地部署 Windows 2000。对于部分公司而言，初始的先导测试项目就是他们投入使用的第一个阶段。其它公司可能会删除先导测试项目安装，然后重新安装以开始生产应用。

在生产应用阶段，主要工作就是反复的部署、测试、验证和支持循环，所以测试和支持活动依然很重要。在部署完成阶段点，新的 Windows 2000 Server 和 Windows 2000 Professional 基础结构被正式转交给运营和支持组。现在该进行项目回顾了。在这一阶段您可能需创建的主要阶段点和部署文档包括：

- 生产应用计划。
- Windows 2000 Server、Windows 2000 Professional 的发行计划。
- 运营和支持信息系统（知识库、步骤以及性能支持过程，包括测试结果和测试工具）。
- 负载或图像设置及安装脚本。
- 文档库（对包括部署记录在内的所有项目文档的软、硬拷贝进行存档）。
- 用于最终用户、管理员、帮助中心和运营人员的培训材料。
- 项目终结报告。
- 灾难恢复计划。

在部署完成、并完成了递交给主管部门的终结报告后，您可能会决定进行项目回顾。可以通过项目回顾对整个项目的优点和不足之处进行客观地评估，并分析如何利用从亲身经历中获得的知识来改进未来的基础结构部署。

部署方案

每个公司都将根据其自身的业务需要和项目管理步骤来创建一个独特的项目规划。以下方案提供了几个企业级单位示例，表明如何将目标转化为阶段点和绩效衡量标准。这些方案是根据参与 Joint Development Program for Windows 2000 的公司的经验制定的。

方案 1：跨国金融服务集团

这个集团拥有九个截然不同的营业公司，每个公司有自己的 IT 部门，但没有公用的 IT 标准。作为一个集团，他们遇到过有关安全策略、域结构以及网络配置方面的问题。目前大多数服务器都在运行 Microsoft® Windows NT® Server 4.0。他们希望达到的主要目的是创建：

- 一个具备 Windows 2000 功能的新 IT 环境。
- 一个九个营业公司公用的目录。

部署小组明确了几个决定部署方案的关键问题，如下：

- 阶段 1：评估
- 阶段 2：设计与工程实施
- 阶段 3：测试
- 阶段 4：迁移（部署）

阶段 1：评估

在评估阶段，每个公司的 IT 管理层就需要一个公用的名称空间问题达成一致。尽管已经有几个公司注册了域名系统（DNS）名称，但问题在于如何找到一个所有公司都可以使用的根名称。这个“占位符”名称需要满足下列条件：

- 精确地定义所有九个营业公司的目录树的根。
- 对于该单位而言应该是一个新名字（任何一个营业公司都没有在内部或外部使用过）。

IT 管理层确定了全局工程组，该组分为八个工作小组，他们会根据一个基本配置规划为每个营业公司进行测试、修改和自定义。表 2.2 显示了各个部署小组及其职责。

表 2.2 部署规划小组

部署小组	侧重点
服务器与基础结构设计	负责整体设计、反复设计与最终工程实施。
Active Directory	主域之下的域和目录树设计以及各自域中的 Active Directory 的持续管理，尤其是与安全性和管理权利有关的管理。
移动与桌面设计	为所有桌面和便携式电脑开发 Windows 2000 配置并确定适当的用于管理这些配置的组策略和 Microsoft IntelliMirror 功能。
安全设置	权限、组成员身份以及管理委派（就有关组织单位设计问题为 Active Directory 组提供情况）。
迁移	将 Windows NT Server 4.0 迁移到 Windows 2000 Server 环境。侧重于并行域临时阶段中的互操作性、迁移和共存，直至迁移完成。
证书服务	文件加密和 PKI。
独立客户	为独立客户开发 Windows 2000 配置并确定适当的组策略和 Microsoft IntelliMirror 功能来管理这些配置。
应用程序管理	确保所有内部应用程序都与 Windows 2000 徽标相兼容。为桌面和便携式计算机确定最佳的部署手段（使用内部开发的推送应用程序或 Windows 2000 安装工具）。确定共享的运行时组件。研究系统文件保护机制。并行地运行现有的应用程序以减少维护。

部署小组通过以下各个方面来确定业务和 IT 需求是否得到基本实现：

- Active Directory
- 新建域设计
- IntelliMirror
- 分布式文件系统

- 磁盘配额管理
- 远程 OS 安装
- Active Directory 与 Exchange 目录服务同步

阶段 2：设计与工程实施

这个阶段中的主要问题是决定域根名称是需要通过 Internet 可见或可访问还是只对内部可用。鉴于已经存在一个代表所有营业公司的 Internet 形象，因此 Intranet 名称需要有所不同。创建一个内部根名称作为占位符名称，这样就可以为每一个营业公司创建一个域。对于创建配置、管理和安全设置等问题，每个公司可以自行管理。

他们还利用这个阶段设计和测试每种功能的配置。然后，部署小组共同研究并确定所选的 Windows 2000 功能之间如何相互作用。他们还制作了培训文档并开始制定支持规划。

主要目标

作为向 Windows 2000 迁移的幕后主导力量，Active Directory 和域设计需要满足以下的业务和 IT 要求，使之为所有营业公司接受：

- 需要一个根域，使所有营业公司可以分享一个公用目录。
- 每个业务单位都希望对其整个单位保有完全的管理控制权，包括所有独立的 Windows NT Server 4.0 域和结构，并且要完全独立于任何其它的营业公司。
- 域和目录设计必须足够灵活，要将公司收购、撤消以及现有营业公司的重组可能考虑在内。
- 每个营业公司根据具体需要安排自己的域及该域之下的所有内容。

确定了 Active Directory 设计之后，迁移小组需要考虑计算机复制以及计算机升级的问题。计算机复制是指这样一个过程，为新操作系统的安装创建一种安装和配置，然后将该配置复制到所有安装的新计算机上去。

由于名称空间的决策对于实现公司目标而言十分重要，因此，要成立一个由每个营业公司的 IT 组代表组成的名称空间设计委员会。该委员会的高级管理层和每个营业公司的 IT 部门需要就最终的名称空间设计取得一致意见。他们需要考虑的名称空间设计因素包括：

- 对 Windows 2000 域模型的影响
- 对现有的 Windows NT Server 4.0 名称空间的影响
- 与现有 DNS 名称空间之间的冲突

公司认为，从 Windows NT Server 4.0 升级到 Windows 2000 的过程中，域的设计和 DNS 都是关键的决策点，原因有二：

- 假如所建议的 Windows 2000 域结构能够真实地反映现有的 Windows NT Server 4.0 域结构，那么他们可以从 Windows NT 域直接升级到 Windows 2000 域。
- 如果他们决定使用与 Windows NT Server 4.0 中相同的 Windows 2000 域结构，那么他们需要有两套并行的域结构。在新的 Windows 2000 环境稳定之前，他们还需要保留 Windows NT 环境。

部署小组认为升级或迁移决策将由以下因素决定：

- 现有的域结构

- 现有的功能
- 由于 Windows 2000 而需要实施的新功能

然后，部署小组发现，要决定每个域中将要包含什么，需要首先对以下项目进行分析：

- 对当前 Windows NT Server 4.0 域设计中的问题进行评估。
- 决定在 Windows 2000 域设计中保留哪些 Windows NT Server 4.0 的功能。
- 根据 Windows 2000 新功能对于新的域结构的增值来决定要实施其中哪些功能。
- 确定其 Windows NT Server 4.0 环境是原样的还是经过了（内部开发小组或第三方解决方案提供商或开发商的）修改或自定义。

  例如，该单位利用内部的脚本工具将用户与特定的应用程序联系起来。这个工具执行应用程序发行功能，类似 Windows 2000 中的“Windows 安装服务”，因此需要决定是继续使用这个内部工具还是使用 Windows 安装服务。使用 Windows 安装服务可以降低内部开发成本，因而降低总拥有成本 (TCO)。最后，他们决定使用 Windows 安装服务。

有关 Active Directory 域结构的详细信息，请参见本书的“设计 Active Directory 结构”一章。有关域迁移的详细信息，请参见本书的“确定域迁移策略”一章。

二级目标

他们的二级目标是确定其它对其环境有用的 Windows 2000 功能，但不一定是 Windows NT Server 4.0 的功能。然后，他们制订一个规划，确定这些新功能是否适合于他们的环境。例如，这个示例集团决定下列功能满足其业务和 IT 需求：

脱机文件 通过将个人文件和网络文件保存在本地电脑中，便携式电脑用户在旅行时可以访问网络数据。对于没有在外旅行的最终用户，即使他们所在的 LAN 或 WAN 服务中断，这一功能也可以确保他们可以继续工作，因为文件储存在该用户的本地硬盘驱动器中。

容错分布式文件系统 在分布式文件系统 (Dfs) 中，他们可以创建一个目录树，树中包括了多个文件服务器和文件共享目录，可供一个组、部门或企业共享。这就使得用户很容易就能找到分布在整个网络中的文件或文件夹。有一个容错 Dfs 链接到已经在 Windows NT Server 4.0 基础结构中使用的漫游用户配置文件。文件可以储存在网络上，方便了公司的合作伙伴进行复制。

磁盘配额管理 磁盘配额管理允许公司使用 NTFS 文件系统格式的卷来监视并限制单个用户可用的服务器磁盘空间。他们还可以定义当用户超出了指定的阈值时所作的响应。过去，该单位使用第三方工具。现在他们使用 Windows 2000 的附带工具以降低内部的开发成本和总拥有成本 (TCO)。

远程 OS 安装 该集团已经拥有一个改进的脚本进程，但每当基本的客户计算机配置改变时，都必须更新脚本。他们将使用 Windows 2000 远程 OS 安装服务来部署 Windows 2000 Professional 的初次安装，并使用远程 OS 安装服务对有故障的计算机进行快速更新。他们计划将远程 OS 安装服务和 IntelliMirror 结合使用以加速并简化计算机的替换，从而降低 TCO。

集成了 Active Directory 的 Exchange 目录服务 该单位计划使用 Active Directory 连接器 (ADC) 使 Exchange 5.5 目录同步，当该单位升级到下一个版本的 Exchange 时，会最终将目录服务集成进来。

阶段 3：测试

该示例集团设立一个测试实验室进行功能和先导测试。他们希望模拟生产迁移的实际条件。在实验室和先导测试验证了迁移过程之后，就可以开始投入实际运行了。在设计阶段，最初的设计先导测试应交付 IT 人员以便他们测试和改进设计。

他们计划测试和评估的初始设计问题包括：

- Active Directory 设计（占位符域和四个子域）。
- 标准客户配置。

他们的先导测试目标包括:

- 在一个真实的生产环境中评估 Windows 2000 和建议的 Active Directory 模型。
- 尽量使用 Windows 2000 提供的新技术。
- 合并标准的客户固定和移动配置。
- 向集团的所有业务单位展示建议的未来配置并收集建设性的批评意见。
- 汇总集团中独立的 Windows 2000 项目并调整其侧重。

在这一阶段，部署小组重新进行设计和测试，直至达成一致意见。新的设计需要满足下列检验标准：

- 提高了稳定性
- 改善了工作环境
- 可以通过当前的、新的或额外的管理资源进行管理
- 满足预算需求

域设计测试并最终完成之后，集团内的每个全局工程小组都将在域设计上签字交付。然后，该设计必须经过所有九个营业公司的高级 IT 管理层的批准。

阶段 4：迁移

由于该单位发现有必要为移动用户保留漫游用户配置文件，他们决定在过渡期间保留两个并行的环境。许多在家里已经升级到 Windows 2000 的漫游用户将发现他们的网络环境还没有升级。但如果保留了并行环境，则不管用户使用什么操作系统，基础结构将支持所有的用户并允许他们访问自己的文件。

但是，迁移仍需要尽快实施。该集团计划将 Windows NT Server 4.0 和 Windows 2000 双系统环境保留 12 到 24 个月。用户将可留在任何一个环境中，直到所有九个营业公司的 IT 环境都完全转变为 Windows 2000。

对于这个集团而言，折叠 Windows NT Server 4.0 环境对于整个迁移过程而言是最关键的决策点。他们希望确信已经进行了足够的实验室和先导测试以减轻由于设计不善而可能产生的严重后果。他们希望通过进行足够的测试来避免导致网络停工。完成测试之后，他们将在所有营业公司中进行 Windows 2000 迁移，然后折叠 Windows NT Server 4.0 环境。

方案 2：跨国消费品和工业品制造商

方案 2 是针对一个高度分散的具有分布式 IT 环境的商业组织，其拥有 175 个不同的营业公司。其制造和组装中心分布于 6 个洲的 49 个国家。他们在全世界拥有大约 390,000 名雇

员，讲 120 种语言。因此需要一个通用的接口和实施过程，以降低所有营业公司的转变难度并降低部署支持成本。所有营业公司都希望解决下列共同的问题：

- 使消费者能够很容易地访问与公司及其业务相关的信息。
- 通过创建一个目录林，降低 IT 管理成本并改善服务。
- 合并基于 Windows NT 4.0 的服务器以便进行升级。
- 为所有营业公司提供一个共同的 IT 环境。
- 为整个组织确立 Windows 2000 部署方针，以提供一个稳定的 IT 环境并防止单个小组部署中央 IT 部门不支持的产品或功能。
- 在所有营业公司之间交流 IT 问题。
- 有效地设计 Active Directory，因为它能够启用 Windows 2000 的许多其它功能。

部署小组

该组织创建一个开发小组，其中包括一个服务器小组，一个客户小组。每个小组都有来自每个主要营业公司的代表。他们的目标是为服务器和客户操作环境开发一个可以由所有营业公司使用的模型。同样，他们的目标是建立并验证一种可以为所有营业公司所使用的设计和部署过程，而不仅仅是在一个生产环境中部署 Windows 2000。他们的计划分三个阶段：

阶段 1：基础结构骨干设计和开发

- 为主要的公司域建立核心服务
- 在公司的主要办事处部署服务器

阶段 2：营业公司的部署规划

- 在所有营业公司建立先导测试域
- 配置站点和站点链接桥
- 创建用户帐户
- 在 Windows NT Server 4.0 和 Windows 2000 域之间建立信任关系
- 在多个营业公司中进行 Windows 2000 Professional 先导测试

阶段 3：将主要服务从 Windows NT Server 4.0 迁移到 Windows 2000 Server

- Windows Internet 命名服务 (WINS)
- 动态主机配置协议 (DHCP)
- 打印
- 使用 Windows Internet 信息服务 (IIS) 的 Web 服务器

该小组首先完成的任务之一是为整个项目创建一个主要需求和风险列表。这个列表包括：

- 认识到建立一个全球性企业所需的协作是前所未有的。（在所有营业公司中为服务器和客户部署操作系统平均需要三年的时间。）

- 根据需求，做好准备与 UNIX 和大型机业务线应用程序共存。（例如，许多营业公司拥有 Sun RISC 6000 服务器，其中包含运行在 Windwos NT Server 4.0 操作系统上的会计程序。）
- 根据公司内部变更和经常性的收购、合并以及撤消，提供移动和合并的工具。

招聘第一个域管理员，他/她应该：

- 对更改需求和根域支持作出响应。
- 能够有效地委派子域和创建站点。

- 认识到一个方案可能无法满足所有营业公司的配置需求；因此，可能需要一个用于公司之间的互操作的目录同步工具。

认识到公司网际协议（IP）的依存关系，如：

- 防火墙
- 网络性能

服务器部署小组

服务器部署小组的职责是根据整个部署小组确定的阶段，规划和设计服务器部署过程。它进而被划分为集中致力于技术规划、Active Directory、后勤以及迁移等若干小组。服务器小组的战略目标是：

- 明确所有营业公司均可使用的 Windows 2000 Active Directory 服务。
- 制订由当前的 Windows NT Server 4.0 环境向 Windows 2000 环境的迁移计划。
- 制订短期内准备步骤。
- 实现企业基干先导测试。
- 对所有的营业公司贯彻指导方针并实施 Windows 2000 模型。

图 2.3 说明服务器小组在部署 Windows 2000 时使用的项目管理框架。

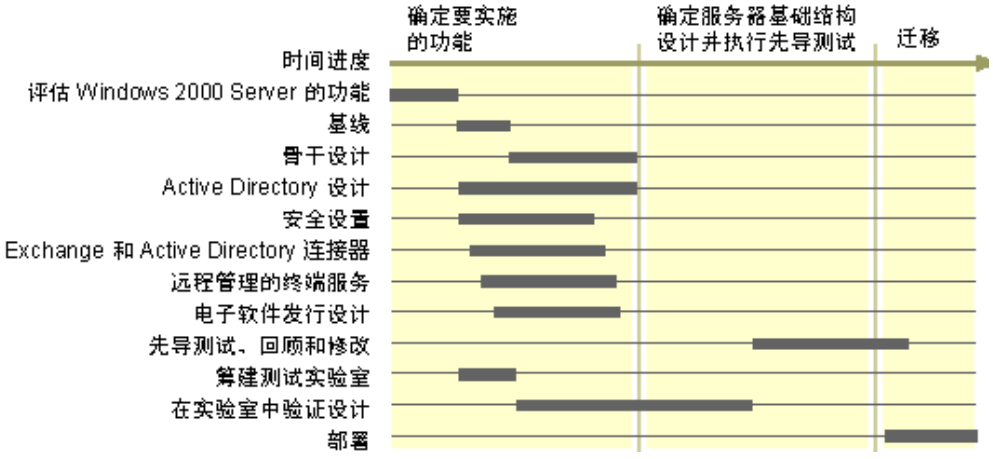


图 2.3 跨国制造商的服务器部署过程

服务器阶段 1：确定实现哪些功能

服务器部署小组的首要目标是为所有营业公司共同的目录和域模型创建部署标准。他们同样需要建立一种全局性 Windows 2000 基础结构以支持所有的营业公司。首先，小组集中致力于通过世界范围内现有的主要企业 IP 基干节点，设计一条基础结构基干。此基干是指根名称空间和域控制器的逻辑基干，而非物理存在的网络基干。通过 Windows 2000 基础结构，他们需要开发一条所有营业公司都可以参与的基干。每家营业公司都要与目录林根接口，并且共享公用全局编录。

然后，基于业务需求，小组开始确定企业具体需要哪些技术。例如，由于在世界范围内所有系统管理员都使用英语，因此服务器级不需要多语种功能。他们需要考虑的具体问题集中在：

- 设计域和站点
- 设计组织单位
- 确定使用 DNS 或 WINS 名称解析
- 理解 Active Directory 复制和容器
- 使 Exchange 目录服务与 Active Directory 同步
- 设计 Windows 2000 的 Active Directory
- 为常规的服务器操作系统配置制订标准
- 确定域控制器和全局编录的放置标准及位置

表 2.3 是公司判断服务器小组是否已实现阶段 1 的目标时的行动清单。

表 2.3 阶段点 1 完成清单

完成	项目
	至少在三个位置建立四到六个服务器的先导测试。
	获准使用 <*域名*>.net/<*域*>.int 作为根域名。
	在指定数目的现有企业 IT 节点安装 Windows 2000 Server。
	确定 <*公司.XXX*> 的 DNS 结构，包含：
	为位于欧洲 *X* 位置的 <*公司.XXX*> 域配置集成的 DNS 动态更新服务器。
	在美国 *A* 位置配置集成的 DNS 动态更新服务器。
	以新建域信息更新核心 IT 服务器。
	通过核心操作站点验证记录串行化和区域复制。
	在*某年/某月/某日*启动 <*公司.XXX*> 的 Direct Host。
	确定核心操作配置，包含：
	在欧洲 *X* 位置和 *Z* 位置建立全局编录。
	标识子网。
	创建 *X* 个站点。
	在欧洲 *X* 位置和 *Z* 位置之间建立站点链接。
	通过为远程管理安装 Windows 2000 终端服务，增强管理能力。
	通过配置基干站点将 Windows 2000 构件复制到欧洲 *Z* 位置，启用电子软件分发。
	在先导测试方案中创建目录服务须通过：
	以企业目录数据（200,000 多个名称）填充先导测试的目录服务。
	验证系统中复制和加载是否成功。
	测试后删除填充数据。

服务器阶段 2：准备服务器体系结构的最终设计并实施先导测试

现在小组已准备进入阶段 2，并开始为先导测试建立各种营业公司域。有些是新建域，而其他则由 Windows NT Server 4.0 迁移而来。他们需要考虑的具体问题集中在：

- 设计 Active Directory 结构并在测试实验室中验证其有效性。
- 制订由 Windows NT Server 4.0 向 Windows 2000 Server 的迁移计划。
- 为服务器部署开发标准安装过程。
- 建立企业集成实验室。
- 为其他的 Windows 2000 功能定义规范。
- 启动最终用户通信计划，涉及其他营业公司中的 IT、 IT 管理员以及桌面用户。

表 2.4 是公司判断服务器小组是否实现阶段 2 的目标时的行动清单。

表 2.4 阶段 2 完成清单

完成	项目
	标识 10 个先导测试位置，其中四个在美国，五个在欧洲（其中一个是欧洲客户实验室）。
	在先导测试环境中部署 18 到 24 个服务器。
	在先导测试环境中部署 30 到 40 个工作站。
	通过在营业公司和适当的企业基干位置之间，为虚拟专用网络 (VPN) 访问配置防火墙，以配置经过 VPN 的企业 IP 基干。
	确定管理委派，包含：
	为营业公司预先创建域。
	委派营业公司进入 DNS 区域。
	为营业公司创建域，包含：
	在欧洲的五个位置和美国的四个位置安装营业公司域。
	标识参与的营业公司子网。
	创建站点并委派站点管理权。
	在营业公司站点和基干站点之间创建站点链接。
	在每一个参与站点（不是营业公司）建立全局编录。
	确定每家营业公司的委派，包含：
	在营业公司域内创建单位部门结构。
	委派单位部门管理权。
	为服务器和客户部署小组的成员确定并创建用户帐户。
	将属于 Windows 2000 部署小组的客户计算机附加到营业公司域中。
	为营业公司建立 Windows NT Server 4.0 信任关系作为工作资源域。
	根据需要在营业公司基干中集成 WINS。
	通过在每家营业公司配置 Active Directory 连接器并通过单向同步更新 Active Directory 信息，集成 Microsoft® Exchange Server。
	创建证书颁发机构。
	创建目录服务复制。
	配合客户部署小组，部署 Windows 2000 Professional 须通过:
	在不同的域中执行客户样机的无人值守安装。
	在所有的域中为客户使用组策略。
	在客户样机上安装三种示例语言的多语种包。
	启用国际客户漫游。
	在基于组策略对象的所有站点安装并使用每家营业公司的标准软件。

	确认工作站可以通过现有的 Windows NT 4.0 远程访问服务访问基于 Windows 2000 的资源。
	定义用户须通过：
	在所有的域中为客户使用组策略。
	确认用户在不同的域中漫游时运转正常（客户端默认语言须相同）。
	确认用户在国际漫游时运转正常（不同的客户端默认语言）。
	确认在世界范围内不同的域中可以进行资源访问。

服务器阶段 3：向营业公司提交迁移规划

阶段 3 的重点在于将服务由 Windows NT Server 4.0 向 Windows 2000 迁移。服务迁移将按照为降低对现有工作系统影响而设计的风险评估进行。小组在迁移关键组件获得部分成功的同时，复杂程度将愈来愈高，风险也随之上升。部署小组在完成全面测试之后，将向营业公司提交规划作为原型。此阶段的活动包含：

- 提交迁移策略。
- 向营业公司介绍 Windows 2000 的概念和设计提议。
- 向管理决策者（IT 评审委员会）推行设计提议。
- 向最终用户推行项目和设计提议。

  准备故障恢复规划以确保业务连续性，特别是：

  - 备份策略
  - 在向 Windows 2000 迁移后，Windows NT 4.0 的恢复（回退）策略

表 2.5 是公司判断服务器小组是否实现阶段 3 的目标时采取的行动清单。

表 2.5 阶段 3 完成清单

完成	项目
	在包含北美、欧洲和亚洲在内的多个物理位置中确定站点迁移的位置。
	为每个域和每个站点确定要迁移的服务器的数目。
	为每个域和每个站点确定要迁移的客户计算机的数目。
	在现有环境中合并 Windows 2000 WINS 服务器实施 WINS 迁移。
	在现有环境中合并 Windows 2000 DHCP 服务器实施 DHCP 迁移。
	选择一定数量的不用作 Windows NT Server 4.0 域控制器的打印服务器升级为 Windows 2000，以实施打印服务器迁移。
	通过使用 IIS 5.0 实现一个 Windows 2000 部署 Web 站点和从现有的中心站点创建指针，以实施 Internet 服务器迁移。从试用站点向新建站点复制目录副本。向服务器添加 DNS 记录。
	将选择的 Windows NT 4.0 资源域向 Windows 2000 Server 迁移以减少资源域。
	将 Windows NT 4.0 帐户域主域控制器迁移到 Windows 2000 Server 以新建帐户域。

客户部署小组

对客户部署小组而言，最大的挑战在于他们与所有的营业公司一起工作，要使一种客户计算机配置获得一致满意。单位中现有的客户操作系统包含 Windows 95、Windows 98、和 Windows NT 4.0 Workstation。小组需要考虑的其他客户问题是：

- 减少在公司范围内使用的应用程序的数目。当前的 1,000 或更多个应用程序使得 IT 小组难于提供支持。
- 使得 IT 的焦点由移动的计算机转移到移动的用户。
- 研究是否更改在 Windows NT Server 4.0 上部署软件的现有方法。
- 为膝上型计算机提供更多的硬件支持。

小组需要提出建议，帮助营业公司决定他们的客户和服务器基础结构谁首先被升级。当小组意识到两种选择都有可能时，小组成员认为对单位而言，当赞成首先更新服务器基础结构时，如下问题相当中肯：

- 对客户计算机实行更为集中的控制。
- 限制用户修改客户计算机配置的权利。
- 使用 Windows 2000 工具进行安装。
- 启用所有用户都可以访问的全局编录。

小组发现集团中的大多数营业公司都愿意首先升级他们的服务器，然后在启用了 Active Directory 和全局编录之后，再为更多细化的客户计算机管理实现组策略、其他更改和配置管理工具。他们同时认识到当小组规划为软件部署推荐使用 Windows 2000 组策略时，服务器是否首先升级就显得尤为重要。小组将需要研究组策略的使用将如何影响 Active Directory。

有单位向客户体系结构小组提出了如下目标：

- 为所有营业公司规划标准客户配置作为模块化的产品。
- 创建包含硬件、软件和操作在内的基准安装。
- 设计适用于全局模型的结构，允许用户从世界上任何位置登录。
- 为培训和桌面帮助支持开发模型。

客户小组的工作可以划分为两个阶段：

- 阶段 1：客户标准配置问题
- 阶段 2：软件后勤

阶段 1：客户标准配置问题

为迎合营业公司在世界范围内的业务目标，客户小组决定使用标准化配置。它包含：

- Windows 2000 Professional 客户程序
- Microsoft® Office 97 或 Office 2000
- 病毒扫描功能
- Web 浏览器
- 电子邮件客户程序
- 多语种功能
- Windows 终端服务功能（确认客户设计适合于终端服务）。

启用国际客户漫游，使得用户可以从世界上任何位置连接到或拨号到企业 IP 基干，并且访问：

- 个人桌面和应用程序设置
- 在任何位置都可以使用个人文档和邮件
- 企业级标准软件。

阶段 2：软件后勤

在阶段 2，小组着重于制订策略，以稳定而有效的方式为固定和移动客户收集新操作系统和客户配置信息。小组确定如下问题：

创建安装软件包为：

- 企业应用程序。
- 所有营业公司的公用应用程序。
- 每家营业公司的自定义应用程序（根据需要）。

为安装软件包创建指南，包含：

- 适用于所有营业公司的标准化软件包开发。
- 适用于非标准软件并针对具体应用程序的特殊安装软件包。

- 根据每家营业公司的需要将应用程序重新打包。

分配安装软件包：

- 所有用户。
- 按职责或单位划分的用户组。
- 客户特定需求。

- 基于用户请求安装应用程序

客户部署小组已经发现管理人员希望随着购买新的硬件，不断地安装新的客户操作系统和配置映象。该集团部署一次操作系统平均需三年时间。内部 TCO 研究表明预先为较高级硬件增加投资，然后升级新的客户配置映象，再将新硬件安装到用户系统中的作法将降低 TCO。

而且，对系统管理员和 IT 专人员而言，显著的客户利益是基于新的功能和增强的性能。然而，用户和经理需要看到有切实的证据表明生产力有所提高。因此，每家营业公司在项目可以进行到部署阶段之前，都要求管理决策者和最终用户进行大批采购。

技术依存关系

由于 Windows 2000 Server 是一种通用的网络操作系统，它由各个独特而整合的功能组成，可以逐步部署，因此在您部署规划之时，有大量的技术依存关系必须考虑。下面的例子举例说明了一些依存关系。

Active Directory 和域名空间

您的 Active Directory 结构和域名系统 (DNS)，连同您为 Windows Internet 名称服务 (WINS) 指定的基础结构规划，动态主机配置协议 (DHCP)，网络协议，文件，打印，数据流媒体以及其他耗费带宽的应用程序都必须设计为适应业务要求和 IT 功能。如果您的业务需要指导大量的子公司，漫游或远程访问用户，那么应考虑组织单位，组策略，安全性和 IntelliMirror 等技术。如果您希望提供安全的内部网或外部网功能，那么 IP 安全措施 (IPSec) 和 PKI 是设计的重点组件。

如果您将 Windows 2000 Professional 部署为桌面型和膝上型计算机的主要操作系统，那么您可能需要考虑安装选项、多语种功能、安全性、Active Directory 以及其他更改和配置管理技术。最后，如果您处在包含除 Windows NT 或 Windows 2000 以外的网络操作系统的异机种环境中，您将需要考虑互操作性和共存选项。

Active Directory 和 Exchange Server

您可能正在规划将 Active Directory 部署在物理分散的环境中，此时由于低速的 WAN 链接使得集中的 IT 管理变得困难，然而仍存在着巨大潜力使稳定而安全的连接成为现实。也许，您的业务要求还需要能够横跨包含物理远程站点在内的不同营业公司，稳定、安全而且通用的电子邮件和协作系统。您需要根据组策略、IPSec 和虚拟专用网络 (VPNs)，考虑 Active Directory 和 Exchange Server 5.5 目录服务之间的关系。规划使用 Active Directory 连接器 (ADC) 保持您的数据与 Exchange 目录同步。

特别是如果每个单位、子公司营业单位都拥有各自 Internet 域名、域和树结构、安全要求以及不同的网络操作系统或 IT 标准时，那就必须考虑 DNS 设计。如同许多以 UNIX 为中心的 IT 部门一样，当是各部门而不是 Windows 2000 小组负责 DNS 名称空间时，DNS 设计会显得尤为重要。

集成 Exchange Server

如果您所在的单位不使用 Exchange Server 5.5，而您又需要共同的电子邮件标准和公用目录时，您可能需要在部署 Windows 2000 之前实现 Exchange Server 5.5，以便您可以使用 ADC 使 Active Directory 同步。或者，您也可以暂时降低目标直到在完成了 Windows 2000 部署后部署下一版本的 Exchange。

远程 OS 安装

另一个例子发生在只能获得有限支持，但是连接性极好的用户场所，在过去那里的本地客户安装由手动维护。使用远程 OS 安装和 IntelliMirror 技术，现在您有机会远程安装和疑难解答，而无需亲临现场进行支持。

在本书的技术规划各章中可以找到有关技术依存关系的更多信息。请谨记，您希望部署的每种功能都需要拥有自己的设计，以便可以在实验室和先导测试的环境中可以被正式地测试。

规划 Windows 2000 部署的窍门

当创建规划文档和详细叙述部署规划时，您最终的目标就在于运用您单位行之有效的项目管理技术成功地部署 Windows 2000。下面章节提供了在部署规划时需要考虑的项目列表。

最佳常规实践方案

下面列表包含由一些 Windows 2000 的早期使用者确定的最佳总体实践方案。

- 查看单位组织框图，了解单位中的管理结构与单位的需求以及网络 LAN 链接相匹配的程度如何。基于这些考虑建立 Active Directory 基础结构。

- 确定国际功能要达到的等级以及为实现该目标愿意采取的折衷方案。
- 在测试您的产品时为额外的复杂级别安排时间。
- 围绕 Windows 安装服务规划您的应用程序设置。
- 确定如何分解应用程序的系统管理职责以及谁将拥有管理权限。
- 确定在典型的用户系统中实施何种策略。
- 利用 Windows 2000 提供的新组件。明智地集成这些组件以最小化他们对应用程序性能的影响。
- 安排足够的时间安装 Windows 2000 Server，它需要几个小时。
- 向 Windows 2000 问题列表和测试跟踪系统中添加国际问题。
- 组成“ 工作组 ”研究基于任务的体系结构决策。
- 撰写完善的测试规划，并且建立测试实验室，按照使用中的硬件和软件类型确切模拟您的工作环境。
- 首先保守地升级。在开始获得成功后可以加快进程和部署速度。

部署阶段

确定在单位中部署 Windows 2000 的最佳整体顺序。有公司使用如下顺序：

- 通过确定单位中当前使用哪些服务器和客户操作系统，以明确当前的环境。研究它们的功能和用途。
- 研究用户的数目是否可能由于合并、收购、重组或发展而变更。
- 研究需求决定服务器环境的规模（确定对群集、负载平衡和终端服务的需求）。
- 设计包含 DNS 名称空间在内的 Active Directory 结构。
- 将网络基础结构和成员服务器升级。
- 实现 Active Directory 和存储管理。
- 将客户升级或迁移到 Windows 2000 Professional。
- 通过更改和配置管理工具实现桌面管理。

应用程序安装问题

当您在单位中计划安装应用程序时，可以使用如下规划窍门。

- 在安装创作过程中进行早期投资。在产品开发周期的早期花时间安排安装过程。
- 开发者参与到安装创作过程。这将有助于早期发现依存关系。
- 请注意 Windows 安装服务验证可能影响您的应用程序的性能。
- 应尽可能避免在安装过程中重新启动系统。
- 请勿向 Win.ini、System.ini、Autoexec.bat 和 Config.sys 中添加语句。
- 要求应用程序的每名测试人员都使用 Windows 安装服务安装这些程序。

- 请谨记管理员可以在未完全安装您的产品的情况下，可将其加入用户的开始菜单或桌面。当用户双击快捷方式或应用程序可支持类型的文档时，应用程序将被安装。
- 理解并规划“ 系统文件保护 ”问题。

国际化问题

如下窍门可以帮助您规划国际安装。

- 应避免假定您的应用程序所运行的操作系统的语言版本。
- 应避免假定区域设置、代码页和用户界面与给定的用户或计算机相匹配。
- 使用 Windows 安装服务。ANSI 和 Unicode 编码都可使用。
- 确定需要哪些字体。很多时候支持国际功能所需的只是安装正确的字体。
- 使用最新的 Windows 2000 打印机驱动程序。它们可以为国际功能提供最佳支持。
- 在跟踪国际化问题时，您的应用程序和操作系统都应进行检查。

性能问题

维持高性能是大多数部署的重要目标。如下窍门可以帮助您规划改善性能。

- 尽可能推后启动时的初始化项目。
- 简化启动屏幕，使得在网络间传送的图形位较少。
- 规划网络中断和常规网络性能问题。
- 使用缓存层，Windows 2000 在共享脱机时为它的文件系统提供该缓存层。

漫游用户和终端服务

如下窍门将帮助您规划漫游用户和终端服务的安装。

- 如果您仔细地规划漫游用户方案，那么终端服务的基本部分就已经实现。
- 支持漫游用户配置文件和状态分隔。
- 从每计算机设置中区分每用户设置。
- 对于每计算机设置不需要写权限。
- 请谨记 Windows 2000 的常规用户只可以修改用户配置文件中的数据。您的应用程序不可以更改注册表中 HKEY_LOCAL_MACHINE 的子树部分。
- 在以用户身份（而非管理员身份）登录时运行您的应用程序，并在用户不具有管理权限的计算机上测试该程序。这将有助于早日发现问题。

管理

在创建规划时，您可以使用如下管理窍门使 Windows 2000 的安装易于管理。

- 确认您的应用程序在保证提供完整功能的同时，管理功能应尽量简化。这将有助于在未开发自定义工具的中小型单位中部署应用程序。

- 在您的应用程序中支持脚本。一种策略：您可以为 Windows 管理规范撰写提供程序，以便花费不多就可以提供简单的脚本支持。
- 支持 OnNow/ACPI 要求处理睡眠和唤醒的通知和请求。
- 请谨记对常规用户而言，默认的安全设置较之 Windows NT 4.0 要安全得多，Windows NT 4.0 可能会要求常规用户在 Windows 2000 中加入 Power Users 组。

规划任务列表

表 2.6 总结了在您创建 Windows 2000 部署路线图时需要执行的任务。

表 2.6 部署路线图任务列表

任务	所在章节
确定项目管理流程，制订适合于您所在单位的关键性阶段点和指标。	制定项目规划流程
在确定需要部署哪些特定功能时，研究它们与其他 Windows 2000 功能和技术之间的技术依存关系。	功能设计与开发
确定哪些项目管理限制将影响部署。例如，财政和人力资源限制，以及假期安排和年终财政问题等单位后勤。	确定目标
制订风险评估过程及准备全面的风险分析。	确定目标
确定部署阶段的顺序。	部署方案
为单位创建项目规划，重点在于 Windows 2000 功能、部署小组、日程安排以及相关的依存关系。	部署方案

有关项目管理的更多信息，参见 Web Resources 页的 Microsoft Solutions Framework 链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

第 3 章 - 部署规划

当您确定用于部署规划的项目管理结构后，就可以开始规划的细节工作了。本章提供有关如何创建项目规划中特定部分的信息。比如说，项目经理需要确定人员需求、部署组、要创建的部署文件类型、差距分析和功能规范。

尽管 Microsoft 认为本章所描述的方法有助于部署的成功，这些推荐的方法仍可以根据您单位的需要和结构加以修改。

本章内容

细化项目规划
测试和先导测试 Windows 2000
创建项目规划文档
Windows 2000 部署
部署规划任务列表

本章目标

本章将帮助您撰写下列规划文档：

- 项目范围和目标
- 人员需求和项目组
- 差距分析
- 行政计划
- 通讯策略
- 教育和培训计划
- 风险评估矩阵

资源工具包中的相关信息

- 有关开发项目规划的详细信息，请参见本书中的“ 创建部署路线图 ”。
- 有关如何运行一个成功的 Microsoft® Windows® 2000 先导测试项目，请看本书中的“ 实施 Windows 2000 先导测试 ”。
- 有关设计测试实验室和评估 Windows 2000 功能的详细信息，请参见本书中的‘ 建立 Windows 2000 测试实验室 ”。

细化项目规划

为了从 Windows 2000 获得最大的收益，需要仔细地规划您的部署。总体项目规划应包含您的业务和技术网络基础结构的各个方面。在开始时，考虑以下部分中讨论的步骤。

项目范围和目标

规划部署的第一步是定义项目目标。您是在这一步中明确希望达到的商业目标以及 Windows 2000 如何帮助您实现这些目标。该策略还将帮助您选择最有用的 Windows 2000 功能。

在项目目标中指出您需要涉及的特定业务需求。包含特定的、短期的目标，比如说，“ 在本商业季度结束之前在 2,500 台计算机上部署 Windows 2000 ”，也应包含概括性的、长期的目标，比如说“ 降低正在进行的软件发行成本 ”。

因为您的目标将影响到您做什么和如何去做，所以在继续部署规划之前应首先确定目标。明确的目标将确保您的规划不至出现偏差。

在记录项目范围时指明您的 Windows 2000 实施将覆盖的地区、功能和环境。比如说，您可能对更新旧的文件服务器感兴趣，而对实施基础结构范围内的 Active Directory 部署不感兴趣。

表 3.1 概述了一些共同的与 Windows 2000 有关的业务需求和项目目标。请注意该表仅是一个例子。您应当评估自己的业务需求来导出自己的目标。您可能发现单一业务需求可能涉及多个项目目标，或者单一项目目标涉及多种业务需求。

表 **3.1**：与 Windows 2000 有关的业务需求和项目目标示例

业务需求	项目目标
通过延长旧系统的生命期来降低总拥有成本。	使用终端服务而不通过升级向系统提供一个 Windows 2000 桌面体验。
使用户更方便的查找和访问网络上的资源。	使用 Microsoft Active Directory 在网络上存储所有目标的信息。
通过提供从多台计算机访问文档和系统信息的能力来支持漫游用户。	使用漫游用户配置文件将桌面设置和文档复制到网络上的某一位置，这样无论用户在何处登录，都可使用自己的设置和文档。

人员要求

组织部署组并给组员分配特定角色。根据您单位的规模和部署的复杂程度，可能还需要创建子组。

评估您的信息技术 (IT) 人员的核心能力。此外，还应评估他们在 Windows 2000 技术方面的能力。然后决定准备如何管理不足之处。下表列出了管理培训事宜时可能需要考虑的问题：

- 在相关人员接受全面的新技术培训之前不要开始部署。
- 外包一部分工作来弥补不足。然后，专门聘请人员对您的职员进行所需技能的培训。
- 将企业的部署、支持和维护外包出去。

重要 一个支持本单位对该项目的总体需求的执行主管对部署的成功至关重要。这个人可以帮助保证部署组理解并完成其目标。

组织部署小组

尽管规划和部署 Windows 2000 时人员需求可能变化，但操作系统部署一般需要几个组员。对于大型组织，中心组中应至少包含两到三个操作系统管理员。而且，必须包含帮助或支持人员。从部署项目之初，就尽量包含对企业了如指掌的人员并让他们大致了解 Windows 2000 及其优点，这有助于满足本单位更广泛的需求。对于国际性组织，建议包括来自其他国家的主要人员。包含受过 Windows 2000 操作系统培训并对您单位的网络环境了如指掌的人员。

一个由安全、网络、互操作性和应用程序测试方面的专家组成的核心组也可以作为他们专业范围内子组的带头人。组员需具有以下能力：面向细节的项目管理能力、丰富的技术经验和创新能力，并能迅速、独立地掌握新技术。组员还需很强的分析能力，能够将项目设想和实现这种目标所需的细节联系起来。

将项目范围和目标文档用做向导，确定哪一个子组将负责规划和测试您希望配置功能的部署。可以考虑将核心部署组分为一个服务器组和一个客户组，然后按照下面的列表将责任委派到子组。

基础服务器组

- Active Directory
- 域名系统 (DNS)
- 网络设计
- 动态主机配置协议 (DHCP) 和 Windows Internet 命名服务 (WINS)
- 安全性
- 管理工具
- Microsoft Exchange Server 和电子邮件

基础客户组

- 诸如 Microsoft® IntelliMirror™、操作系统和应用程序安装和现存的应用程序等客户和桌面功能。
- 关于笔记本电脑和膝上型电脑的问题，如电源管理、插接站、远程访问和漫游配置文件。

对组进行规划以反映您的内部结构、业务需求和希望部署的 Windows 2000 功能和服务，以及部署方式。部署组的组织应反映以上所示的各种角色。

表 3.2 显示了一种组织部署组的方法。

表 3.2：部署组示例

组	责任
总体控制	包含其他所有组的领导来执行总体协调和联络。包含深刻了解本企业的战略计划者，比如说，那些记得现存系统的位置并知道其作用的人。
规划和协调	负责支持和培训、业务规划、迁移前规划、关键任务系统和第三方咨询。

服务器	在以下方面测试和开发解决方案：群集、分级存储管理 (HSM)、备份、灾难恢复、终端服务、集成和硬件需求
基础结构设计	负责域模型、Active Directory、局域网 (LAN) 问题、电信、分布式文件系统 (Dfs)、全局文件访问、域名系统 (DNS) 和远程访问。
安全性	开发用于 Internet、Intranet 和 Extranet 服务以及域安全和策略实现的标准。
互操作性	系统网络结构 (SNA)、与大型机和 UNIX 的 Kerberos 链接、 UNIX/大型机集成，以及 NetWare 和 OS/2 的集成/共存。
应用程序集成	集成消息传递、数据库、工作组应用程序和套件、Internet 工具以及行业和第三方应用程序。
网络	研究、测试和开发目录启用的网络解决方案。
客户	测试和解决应用程序、升级/迁移、硬件和膝上型电脑问题
桌面管理	测试和开发组织的更改和配置管理规划，包括组策略、软件安装及用户数据和设置管理。
建议请求委员会	由来自用户团体的成员组成。对部署组作出的决定提供反馈。

指派 Windows 2000 小组角色

Windows 2000 部署活动分为许多类别。在小型实施项目中，一个人可能承担多个角色；在大型实现项目中，几个人共同承担一个角色。

请记住，如果启动了目录服务，Windows 2000 与未启动目录服务的环境大不相同。 要使用目录服务，应当对 IT 部门进行培训并将其逐渐迁移到新的支持和管理结构。这种转变将影响到整个组织，并要求比典型升级更高层次的管理培训和参与。

表 3.3 描述了当确定人员需求时，应当考虑的关于 Windows 2000 的人员角色、责任、需求和工作量变化。

表 3.3：Windows 2000 管理角色

角色和责任	所需技能
IT 管理或执行主管 为 Windows 2000 基础结构设置优先级。建立项目的业务案例。定义部署设想和保障投资担当组和组织的提倡者。清除障碍，权衡功能与日程安排，并负责通讯规划。	了解组织的商业问题以及 Windows 2000 提供的解决方案。 具有 Windows 2000 Server 和 Windows 2000 Professional 的主要特点和功能的相关知识。
项目管理 促进做出发布 Windows 2000 基	具有 Windows 2000 服务器和 Windows 2000 Professional 功能细节的相关知识。

础结构所必须的关键决定。构思解决方案并同部署组一起定义部署范围。 与其他组员一起创建功能规范。促进日常协调以交付与企业标准和互操作性目标一致的 Windows 2000 系统。促进总体重大权衡决定。	协调执行管理目标与项目组目标的能力。
开发/设计 评估将要用于设计和开发 Windows 2000 基础结构的技术解决方案。为在部署阶段发布的每个 Windows 2000 功能定义策略。在设计最初的基础结构中扮演重要角色。设计和构造实施所需的基础结构。	开发复杂操作系统服务的经验。理解现存的和新的网络基础结构的技术要求。
主题/技术专家 负责设计和开发专业领域的策略。提供对子组的指导。	在其相关领域和 Windows 2000 操作系统方面具有高级技术能力。 面向细节的项目管理能力。
测试 帮助开发初始解决方案设计。保证在产品首次展示之前组成员熟知并开始关注所有问题。在产品首次展示之前设计和构造测试实验室并执行所有测试和验证程序。进行可扩展性分析和性能测试。	熟悉 Windows 2000 Server 和相关网络硬件，或者 Windows 2000 Professional 连接。具有设计、运行和调试测试方面的经验。具有测试应用程序方面的经验。
文档 帮助开发项目文档，包括规划文档、报告和白皮书。可以包括作家、编辑和制作人员。	熟悉相关技术。具有沟通、写作、编辑能力和技术文档知识。
用户教育/培训 作为用户培训倡议者。评估用户需求、确定培训目标、开发教育和培训计划以保证用户最大限度的利用 Windows 2000 基础结构。	熟悉企业的 IT 系统、网络基础结构和 Windows 2000 功能。具有自助解决方案和演示文稿软件的知识。沟通和培训能力。
后勤管理 保证流畅的展示、安装和向操作和支持组的迁移，包括帮助支持和培训。	对 Windows 2000 Server 和 Windows 2000 Professional 的特点和功能有深刻的了解。

当检查管理需求时，可能会发现需要修改现行的组织方式。您可以利用这个机会去了解当前的系统管理方式和改组是否会带来好处。比如说，如果使用了两个单独的系统来监控 Microsoft Exchange 和 Microsoft®

Windows NT®，您可能想创建一个单独的组来监控 Windows 2000。

当前计算环境

在设计 Windows 2000 环境之前，必须彻底了解当前的计算环境。记录现行计算环境将有助于理解您企业的结构及其如何支持用户，而且这种工作将有助于设计 Windows 2000 部署规划。在处理诸如网络布局这样的复杂概念方面，图表是一种非常有用的方法。在适当处创建这些图表并在项目规划文档中包含这些图表。

关于网络图表的详细信息，请参见本书中的“为 Windows 2000 准备网络基础结构”和“确定网络连通性策略”。

当检查现行计算环境时，必须记录以下部分：

商业组织和地理需求 描述您业务单元的位置和组织。大批雇员是分布在广阔分散的地理区域还是彼此位置非常靠近？企业的业务单元之间是彼此紧密相关还是在需求和需要上大相径庭？

关键业务过程 如果正在修改关键业务流程，请加入一些图表，来说明这些流程以及新的 IT 基础结构对这些流程的影响。比如说，在某些组织中，一个关键的 Windows 2000 Server 部署目标可能是使用 Active Directory 将管理职责分配给本地的管理员。通过分配管理职能，管理员可以更好地解决本地用户的需求。在这种情况下，创建一个模型来说明总体规划如何实现该目标。

信息结构 当使用图表表示关键业务流程时，应说明如何在合适的地点和时间获得重要决策所必须的信息。比如说，销售和市场人员是否能够确认用户定单的精确交付日期？在概念设计中，确保这些关键数据的存储组织有序并易于访问。

应用程序需求 列出您组织内使用的所有应用程序的完整清单。包括所有定制（内部）应用程序。在记录计算环境时，还应注意雇员使用计算机所从事的不同任务以及迁移到 Windows 2000 将如何影响他们的工作。比如说，如果雇员正在使用的某种旧的行业应用程序依赖于特定的开放式数据库连接 (ODBC) 驱动程序版本，应对这种行业应用程序进行测试以保证其正常工作。

技术结构 当记录网络结构时，应保证包括拓扑结构、规模、类型和通信模型。任何计划对技术结构，诸如硬件、网络和服务所做的重大修改都应在高级图表中说明。

现行和未来的 IT 标准 许多组织的网络和应用标准随时间变得逐渐零碎和陈旧。这种现象在企业合并和购并其它公司时尤为普遍。构建时间跨度大、设计人员不同、地理分布不一的全异系统将对成功部署构成潜在的威胁。对现存系统的审核有助于部署组的成功。

管理模型 通过检查现存的管理模型，确定 IT 人员在企业各个领域正在执行的管理任务。这有助于确定是否需要改变现存管理运营设计的某些方面来适应某些希望部署的 Windows 2000 功能。

确定标准和指导方针

许多组织发现确定 Windows 2000 标准和指导方针可以节省时间和财力。这是因为标准环境可以减少过多配置组合的可能，并提高管理和建造工作的效率。这些标准取决于雇员使用计算机的方式。比如说，做计算机辅助设计的雇员比使用一般办公应用程序的雇员具有更高的需求。

为了达到最佳结果，应为客户和服务器建立标准配置。对以下部件—CPU、RAM、硬盘以及象 CD-ROM 驱动器和不间断电源等辅助设备—的最低值和推荐值确立指导方针。

确立组织中所使用的标准软件配置。包括操作系统和其他应用程序软件以及有关如何发行、支持和限制该软件使用的指导方针。

为组织中所使用的网络操作系统和协议确立指导方针。包括所有网络组件（如路由器、集线器和中继器）的标准配置。确立支持和维护这些配置的指导方针。

最后，确立 Windows 2000 所需的新标准和指导方针，包括方案管理和跟踪、站点设计和命名标准。

实施差距分析

对现行计算环境和基于项目目标的未来环境进行比较。现行环境与目标之间的差距有助于确定应该部署哪些 Windows 2000 功能。进行差距分析的主要步骤是：

- 确定雇员现在的工作方式和部署完成后您希望他们采用的工作方式之间的差距。

  计算机和操作系统只有对雇员有用时对企业本身才有意义。成功的部署将弥补雇员现在的工作方式和部署完成后新系统使之能达到的工作方式之间的差距。随后，当组开始衡量成功度时，主要的尺度将是系统如何改进系统使用者的工作。

- 如果可能，检查以前计算机和网络升级的文档。除了提供有关现存计算环境的有用信息之外，现存文档还可以为您提供在决策过程中可遵循的模板。

- 检查从硬件或软件供应商那里得到的文档。有关基础结构中现存硬件和软件的文档有助于决定是升级还是取代计算资源。

- 确定任务并决定每项任务所需的资源。确定任务及完成任务所需的资源之后，您就可以决定需要涉及到企业内的哪些组以及是否需要企业之外的额外资源。

- 更新所有文档，如包含计划、工作及资源分配等内容的电子表格或日程安排。时时拥有最新的文档将使计划工作日程和分配资源更加容易。

- 将差距分析文档发送至企业内的有关决策者进行审批。如果获得批准，项目可以开始；如果未获批准，您需要在开始实施之前对文档进行修改并重新送报审批。

本书提供了特定的规划和设计指导方针。

测试和先导测试 Windows 2000

在部署 Windows 2000 之前先在实验室内测试您的 Windows 2000 设计。在规划早期，您需要选择测试和先导测试场所并评估硬件需求。实验室投入运行之后，就可以使用该实验室来更好的理解产品、印证概念和验证解决方案。实验室应随着项目的进行而不断发展。

一般来说，测试计划文档应尽可能详细，以保证测试和部署组得到所需的所有信息。在测试计划中描述范围、目标、方法、日程安排和资源（硬件、软件、人员、培训和工具）。单个组和子组需要针对他们的技术专业领域创建自己的测试计划并撰写测试案例。测试案例描述如何完成测试。这使得重现和比较测试结果成为可能。

在项目早期，测试将集中在组件方面来确认设计。随后测试将集中在组件的互操作性方面以保证所有部分协同工作。需要测试应用程序与 Windows 2000 的兼容性。首先测试那些对企业至关重要的功能和设计修改起来既昂贵又耗时的功能。

应包括一个计划，将出现的问题上报到最能解决该问题的人。一个明确的逐级上报程序有助于小组将注意力集中到解决方案上并采取迅速正确的行动。

如果正在部署 Active Directory，必须提供有目录服务的应用程序测试。

在实验室环境中确认 Windows 2000 部署之后，在开始一般部署之前还应进行至少一个先导测试项目。先导测试项目为最终部署设定基调，所以对项目的各方面做充分的准备是非常重要的。您需要确定安装所需的时间、为加速安装过程所需的人员和工具以及总的日程安排。先导测试提供了一种测试部署规划的方法。先导测试项目还提供了一个培训支持人员和了解用户对产品反映的机会，这样就可以预计支持需求。

有关建立测试实验室的详细信息，请参阅本书中的“ 建立 Windows 2000 测试实验室 ”。有关先导测试的详细信息，请参阅本书中的“ 实施 Windows 2000 先导测试 ”。

注意 在进行全面生产部署前完成先导测试项目。完成先导测试项目的每一阶段后，都要记录结果、确认达到项目要求，如有必要重新修订规划。在进行全面部署阶段前解决所有主要问题。必须保证在先导测试中包括了生产环境的所有方面。比如，对于一个包括多种语言的国际性部署，应保证在先导测试中涉及了国际语言问题。

创建项目规划文档

在部署项目的整个过程中，需要创建一系列文档来定义设想、促进、支持、指导和总结部署过程。无论此信息是包含于几个文档中还是许多文档中，都应包括以下部分所讨论的信息。

管理文档

管理文档是项目规划的一部分。它们有助于确定目的和定义目标。它们使工作井然有序并按时完工。请在管理文档中包括以下信息：

范围和目标 如前所述，应保证规划中清楚地说明了项目目标、定义了范围并提供了评估进度和成功的方法。

阶段和阶段点 建立项目阶段，给员工时间以熟悉情况，并帮助您验证规划阶段所做的假设。至少过程中的某些部分应是重复的。建立和监控阶段点以保证项目未出偏差。有关这方面的详细信息，请参阅本书中的“ 创建部署路标图 ”。

预算 确定和跟踪项目的预期费用和费用限制，包括开发、硬件、设备、培训、人员、测试和部署。落实后备资金来源准备应付未预料到的花费。确保企业对此项目的设想是明确的，这样投资的分配就明确了。

人员配备 规划如何为 Windows 2000 部署地点配备人员。一个概述组织结构、责任、会议频度、通讯策略和总体任务及功能拥有者的文档是很有用的。有关这方面的详细信息，请参阅本章中的“ 分配 Windows 2000 组角色 ”。

设备 确定设备需求并与本组织内的适当组通讯。定义设备需求并尽早获得所需空位以减少这些问题成为部署障碍的可能。

总体风险评估 确定存在于部署之外的项目风险。可能的风险包括资源可用性、即将发生的合并或者关键人员的流失。

通讯策略 通过与组织内的其他组交流您的规划，可以提高部署项目的可管理性和用户对部署项目的了解程度。通过其他经理和关键人员定期审阅您的规划，在项目早期开始构建支持和赞同。有关这方面的详细信息，请参阅本章后面的“ 通讯策略 ”。

部署文档

建议您创建以下部署文档，作为项目规划的一部分。

现有网络环境概述 包括目前网络环境的高级描述，包括网络基础结构、硬件、策略、用户数量和类型及地理位置。

部署设计 详述向 Windows 2000 转变的过程，包括服务器和客户计算机的升级和迁移策略；这些升级将在何时何地如何发生，以及将涉及到何人。将现存系统和应用程序考虑在内，如操作系统的改变对现存应用程序的影响、存储容量和硬件能力。

差距分析 说明现存环境和项目目标之间的特定差距。然后列出支持项目目标所需的特定改变。有关这方面的详细信息，请参阅本章前面的“ 实施差距分析 ”。

容量规划 确定将涉及的问题和或有费用，保证有足够的硬件和网络容量来支持要部署的 Windows 2000 功能（如，Active Directory 或远程操作系统安装所产生的复制流量）。您希望确保关键服务在首次展示期间和之后都不应降级。有关这方面的详细信息，请参阅本章后面的“ 容量规划 ”。

风险评估 确定规划中的风险并开发应急计划，以准备随时应付风险。不断的重新评估部署规划并在完成项目的每一阶段之后做出一个正式评估。有关这方面的详细信息，请参阅本章后面的“ 风险评估 ”。

问题逐级上报规划 确定一个逐级上报路径，企业人员可以利用它根据需要解决和逐级上报问题。将问题或环境的类型与最能处理他们的人员进行匹配。一个逐级上报过程使小组将注意力集中于问题的解决上。

先导测试规划 确定参与首次演示的服务器和客户的目的和目标，将部署哪些特征，以及将采取哪种机制从先导测试参与者那里收集反馈信息。有关准备和实施先导测试的详细信息，请参阅本书中的“ 实施 Windows 2000 先导测试 ”。

测试和部署策略 对如何测试和部署 Windows 2000 进行规划。有关这方面的详细信息，请参见本章前面的“ 测试和先导测试 Windows 2000 ”。

功能规范

功能规范详述将要实施的操作系统功能及其配置和部署方法。所有这些元素都需要与部署项目的范围和目标相结合。

描述用户的不同类型、用户执行的关键任务、这些任务现在的执行方式、以及在新的网络环境下如何提高性能。如果您的组织是一个拥有多个站点的大型组织，或是国际性组织，那就需要地理方面的细节。

Windows 2000 的许多功能是相关的，如果您计划部署 Active Directory 时更是如此。基于这个原因，相依性矩阵就非常重要了，并且可以考虑将其作为一个主要文档。

部署组需要协同工作，以确定集成每一组件所需的任务并估计完成这些任务所需的时间。确定组员和管理层应当了解的所有问题。尤其重要的是确定影响其他小组的依存关系。比如说，您可能会发现多个小组的工作都包含域名系统 (DNS) 结构，因此应当协调他们的任务以避免重复劳动。

通讯策略

详细的通讯规划可以增强部署项目的有效性。恰当的通讯会使规划和部署 Windows 2000 的工作更有可能与其他部署新 IT 项目的小组的工作互相补充和相互集成。这有助于管理层帮助项目组跨越障碍并帮助用户做好利用新基础结构的准备。

有效的通讯策略确定了几种类型受众的需求，如执行管理层、项目组、IT 部门和各种级别的用户。保证人员了解情况可以使他们都参与进来。使用通讯策略来构建对部署项目、Windows 2000 新技术和此技术支持的业务流程的支持。

创建通讯计划时，解决以下问题是非常重要的：

部署信息如何发布？可以使用电子邮件和 Intranet 来补充较传统的媒体，如打印。一个使用户了解情况的最好办法是创建一个容易用部署状态报告更新的 Intranet 站点。充分的自助将加强用户的体验。这会减少混淆，降低支持费用。

将要传达什么信息？解释新基础结构将如何使用户的工作更容易以及它将如何满足企业的商业需求。部署状态是需要传达到用户和部署组成员的重要信息之一。突出成绩，但也应承认障碍。

信息发布的频度如何？对于最终用户，只需每月更新。对于行业经理，更新频度应更快些，尤其是将要进行先导测试和产品展示时。对于 IT 部门的成员，无论其是否直接参与部署，推荐每周更新一次。您所做的更改对 IT 人员的工作方式有直接的影响。他们需要密切关注项目部署的进程。

采取何种方式的反馈机制？详述最终用户反馈规划。创建一种用户可以用来表达他们的需求和挫折的反馈机制对成功至关重要。双向的通讯渠道允许用户成为项目的一部分并作为组成员提供有用信息，这些信息有助于项目的成功。

教育和培训计划

在开始部署之前，对用户进行 Windows 2000 特征和功能方面的培训。您可能还希望提供正式的培训并开发一个反馈机制。

针对 Microsoft Windows 2000 Professional 和 Windows 2000 Server 的 Microsoft Official Curriculum (MOC) 提供了关于部署、管理和支持基于 Windows 2000 的网络方面计算机专业人员培训。该专业技术课程提供以下知识和能力：

- 理解 Windows 2000 的特点和功能。
- Windows 2000 的安装、配置和向 Windows 2000 升级。
- 管理一个基于 Windows 2000 的网络。
- 从 Microsoft Windows NT version 4.0 向 Windows 2000 升级支持能力。
- 设计 Windows 2000 目录服务基础结构。
- 设计 Windows 2000 联网服务基础结构。
- 设计改变和配置管理基础结构。

关于针对 Windows 2000 的 MOC 的详细信息，请参见 Microsoft 培训和认证—位于 http://windows.microsoft.com/windows2000/reskit/webresources 的 Web Resources 页上的 Microsoft Official Curriculum 链接。

容量规划

容量规划为规划和管理计算环境提供一个可靠的基础。一旦确定满足商业需求所需的计算资源，您将获得以下好处：

- 达到服务目标。
- 提高生产力。
- 开发和维持可扩展性。
- 控制和减小总拥有成本 (TCO)。

容量规划中最重要的任务之一是为工作量和计算资源建立一个典型的基线。容量规划者和业务规划者必须协同工作以确定依赖于计算资源的业务元素并预测工作量。资产管理对完成硬件清单非常关键。如果需要替换硬件，在升级之前仔细查看哪些硬件需要替换。

一些企业依赖于经理在容量规划方面的专长，另外一些使用分析模型、仿真、基准、或在关键情况下进行容量规划的实验。无论采用何种技术，计算环境的成功管理都要求一种更积极主动的方法。

一个好的起点是概括每小时、每天和每月发生在网络或子网中的不同动作，如：

- 密码更改的数量。
- 用户登录次数。
- DNS 查询的数量。
- 机器帐户密码更改的数量。

然后，确定以上各项的最小、最大和平均值。您希望知道这些事件发生的次数、在网络上占用的网络带宽和这些事件在服务器上占用了多少处理能力和磁盘空间。

确定这些相同实体在新产品上展示的量。然后可以使用此信息来优化服务器及规划域和站点结构。

有关容量规划和 Windows 2000 功能的详细信息，请参阅本书中有关您正在规划的技术的章节。

风险评估

当您计划部署一个操作系统和网络基础结构时，应当对意想不到的问题做出规划。即使最好的部署规划也会受商业需求的改变、经济、用户需求、或电力中断和暴风雨破坏等等因素的影响。

风险管理规划有助于在风险发生之前确定可能的风险，并在风险确实发生时做出迅速的反应。一个经过深思熟虑的、积极主动的风险管理规划能帮助您：

减小风险因素实际发生的可能性。如果您的职员中仅有一个人对企业安全基础结构有全面的了解，在部署期间失去这位雇员将产生重大影响。减小风险的措施有：为每一名主要专家培训备用人员，保证文档是最新的和可访问的。

如果风险发生，减小损失的量级。如果怀疑 Windows 2000 Server 部署项目预算不足，可以确定几个后备资金来源来弥补意想不到的费用。

改变风险的后果。部署过程中出现的意外重组、商业收购或分离都会严重扰乱您的规划。如果已经建立了应付突发变化的程序，就可以从容迎接挑战，而对项目日程安排几乎或根本没有影响。

为在部署期间减轻风险做好准备。可以通过在战略上规划安装和初次展示来达到此目的。比如说，先向现存的 Windows NT 4.0 域中添加新的 Windows 2000 域控制器。或者是构建新的 Windows 2000 域，建立与现存帐户域的信任关系，然后复制用户帐户。或者，可以在域内安装新的 Windows NT 4.0 域控制器，将其移

至专用网，然后对其升级以安装新域。这里的每一个例子中，都可以根据需要很容易地返回到上一个环境。

风险管理

为了有效管理风险，您的风险管理规划应当：

- 确定关键任务应用程序。
- 确定和分析潜在的风险。
- 量化风险的潜在影响。
- 详述逐级上报过程。
- 确定解决方案。
- 与高级管理人员和项目成员交流。
- 成为日常项目管理的一部分。
- 保证最新。

风险管理应是小组定期活动的一部分并涉及所有关键人员、过程、业务和 Windows 2000 部署的技术方面。您需要：

评估有可能影响项目的各方面风险。要求每一组确定和管理与其职责范围相关的潜在风险，如安全、网络、设备、支持或培训。

区分风险的优先次序。风险依严重性和可能性而不同。确定哪些风险对企业的威胁最大。首先处理主要风险因素。

与支持行业现存应用程序的人员接洽。旧的行业应用程序会带来特殊风险。尽早与在这些应用程序方面有丰富知识的人员接洽。如果第三方负责这些应用程序中的一部分，应尽早将其纳入流程中。

避免仅仅基于未包括的风险数量做出生存能力的判断。一个具有 20 个确定风险的项目未必比一个具有 40 个确定风险的项目更稳定。一个确定了更多风险的评估仅比一个确定了较少风险的评估更彻底。使用该文档查明那些对项目有严重影响的风险以及那些有较小影响的风险。

促成一种确定风险的人不受排挤的氛围。企业内从事专业工作的人员经常比他们的上级更早发现问题。如果这些人对汇报坏消息有顾虑，您的风险评估就危险了。可以考虑执行一种奖励机制，对确定风险和为这些风险提供解决方案的人员给予奖励。

风险评估矩阵

为了全面确定潜在的风险，应十分清楚不同部署要素之间的相互依赖关系。一个风险矩阵有助于确定和联系这些要素。

表 3.4 包含一个风险评估矩阵的实例，其中列出了各种问题，如风险发生的概率、某个特定风险对项目的影响程度以及减轻风险所需的策略。

表 3.4：风险评估矩阵样本

风险	概率	影响	所有者	解决日期	缓解策略

正在考虑的合并	中等	高	部署组经理	*年/月/日*	创建一种可以迅速实现与另一企业对等小组合并的策略。
在 Windows 2000 部署之前，并非所有用户都拥有一台达到最低硬件配置要求的计算机。	中等	中等	程序管理、帮助支持和后勤小组	*年/月/日*	决定是在安装时升级硬件还是等待整个企业的硬件升级。

在规划早期创建此矩阵并定期对其进行更新，或者当日程安排、规范、管理、小组、范围或展示策略发生变化时对此矩阵进行更新。

风险驱动日程安排

没有多少部署要素比构思欠妥的日程安排更容易造成风险。比如说，如果您的企业要在第四季度冻结部署，在最后一分钟压缩过多关键步骤可能会降低测试和展示的质量。如果您把最简单的部署要素安排在前，而把最复杂、风险最大的要素排到最后，这样会减少用来解决更复杂问题的时间。

一个考虑了风险评估的日程安排可以减小出现重大问题的可能性。以下的指导方针有助于创建风险驱动日程安排：

在任务等级评估的基础上进行日程安排。从任务等级评估着手，先完成小组的日程安排，然后再综合多个小组的日程安排。在自底向上的任务等级评估基础之上安排日程，会迫使您确定和解决那些可能导致项目延期或使项目脱离正轨的问题。

首先开发高风险要素。首先处理部署中高风险的要素。如果进早处理，由延期、设计更改或其它问题所带来的后果对部署其他部分的影响将减小。

建立主要的和临时性的阶段点。阶段点是一些检查点，这些检查点针对通过测试证实的过程。经常性的临时阶段点有助于在过程中尽早根据新信息重新评估进度并减少错过主要阶段点的风险。

为不可预料情况分配时间。重要部署的完成几乎都会受到那些干扰日程安排的事件影响，如主要人员生病、硬件订货问题或资金问题等。在日程安排中为这些无法预料的环境预留时间。

为项目管理安排时间。定义设想、保证资金和完成其它所有项目管理工作都需要时间。为项目管理安排适量的时间。

使用项目日程安排工具。项目日程安排工具有助于实现任务与从属关系和相关性的连接、迅速确定任务责任人和任务状态。它们还可以用来跟踪不同小组的进程和任务，以保证项目按照日程安排进行。

保证日程安排最新。当业务或部署环境发生变化，增加了新活动和达到阶段点时，应更新日程安排。

当需要改变日程安排时应通知项目领导。定义目标可使职员了解何时停止部署。比如说，如果在十台计算机上安装了 Windows 2000 并且发现一个存在问题的第三方服务，这时可能需要在继续前先解决此问题。

Windows 2000 部署

部署规划的最后阶段是定义如何创建从先导测试到生产的平稳过渡。您的目标是成功、高效地部署 Windows 2000，并将其对用户、网络和企业核心业务职能的影响降到最低限度。

向生产环境部署 Windows 2000 与先导测试阶段部署 Windows 2000 有许多相同之处。一些保证成功的推荐步骤是：

分阶段进行部署工作。增量部署有助于减小风险，并将系统崩溃的可能性降到最低。

创建部署备份计划。在部署过程中出现问题时，一个可靠的、经过测试的备份计划有助于迅速容易的恢复。

创建备份/恢复计划。因为最好的数据保护策略也无法防范计算机和站点灾难，所以应当有一个系统灾难恢复计划。有关创建灾难恢复计划的详细信息，请参见本书中的“确定 Windows 2000 存储管理策略”。

提供适当的培训。保证支持和管理组接受了全面的培训并为部署做好准备。

保证最终用户得到通知。在向最终用户的计算机部署 Windows 2000 之前，先通知和培训终端用户。有些企业要求任何新技术部署之前应首先进行最终用户培训。如果这是一个您正在考虑的策略，应考虑到额外的资源和费用。

保证小组得到通知。保证小组了解以下事宜：部署规划总体、他们的责任和参与范围以及在规划或日程安排方面所做的更改。

安排下班后的主要部署活动。对主要 Windows 2000 活动的周密安排可以把对用户和网络的影响降到最低。比如说，在某一特定组完成最后期限或其他主要项目之前不在此部门部署 Windows 2000。

部署规划任务列表

表 3.5 总结了在规划 Windows 2000 部署时需要执行的任务。

表 3.5：部署规划任务列表

任务	所在章节
定义项目范围和长期、短期目标。	项目范围和目标
筹划 Windows 2000 功能实现项目目标。	项目范围和目标
记录当前计算环境。	当前计算环境
实施差距分析。	实施差距分析
定义人员角色和完成任务所需时间。	人员要求
设置硬件、软件和网络配置标准。	确定标准和指导方针
创建管理文档。	管理文档

创建部署文档。	部署文档
开发部署设计。	部署设计
创建通讯策略。	通讯策略
评估容量需求。	容量规划
确定风险。	风险评估
创建和维护日程安排。	风险驱动日程安排
建立教育和培训计划。	教育和培训计划
开发测试计划。	测试和先导测试 Windows 2000
规划先导测试项目。	测试和先导测试 Windows 2000
规划向 Windows 2000 的平稳过渡。	Windows 2000 部署

第 4 章 – 建立 Windows 2000 测试实验室

在部署 Microsoft® Windows® 2000 之前，即使是在先导测试中，也要确保在模拟并保护生产环境的环境中测试所计划的设计。可以通过设计并实施反映目标环境中的条件的测试，对设计进行验证。

本章为测试经理、以及部署项目组提供了满足您的单位的特殊需求的设计和运行测试实验室的注意事项。同时，本书各章将讲述与 Windows 2000 特殊功能有关的测试问题。

本章内容

开始测试环境
确定实验室策略
设计实验室
建立实验室
管理实验室
测试
部署之后测试
实验室测试规划任务列表

本章目标

- 本章将帮助您创建下列规划文档：
- 实验室说明
- 实验室布局图
- 逐级上报计划
- 测试规划
- 测试案例

资源工具包中的相关信息

- 有关应用程序测试规划的详细信息，参见本书中的“ 测试应用程序与 Windows 2000 的兼容性 ”。
- 有关在生产环境中规划先导测试的详细信息，参见本书中的“ 实施 Windows 2000 先导测试 ”。

开始测试环境

Windows 2000 项目成功的关键因素是彻底地进行基于实际方案的测试。实际方案要求测试环境尽可能模拟真实的生产环境。在这个测试环境中，规划小组中的成员可以验证他们的设想、找出部署中的问题和优化部署设计，同时加强对技术的理解。这些活动减小了出现错误的风险并使得在部署期间和部署之后的生产环境中的停机时间降到最少。

建立测试环境

测试环境包括所有支持测试而不危及企业网络的位置。许多大型单位将测试环境分布在众多的物理、甚至地理的不同位置，以在不同的技术、商业或政治环境中测试。下列因素影响您对测试环境所作的决定：

- 测试方法
- 要测试的功能和组件
- 执行测试的人员

测试环境可能包括一个或多个实验室，而实验室可能包括一个或多个位置。在本章中，实验室这个术语是指设计用于测试的、与企业网络分开的网络。

对于 Windows 2000 项目，可决定将几个独立实验室用于不同的测试目的。例如，可将一个实验室用于网络基础结构和服务器测试，而将另一个实验室用于客户计算机和应用程序测试。相反，单个实验室可能包括多个位置。例如，可将通过广域网 (WAN) 连接多个位置的网络基础结构实验室，用于测试不同链接速度的影响。

如果同时部署 Microsoft® Windows® 2000 Server 和 Microsoft® Windows® 2000 Professional，许多因素影响您做决定：是两个项目分别用两个实验室还是共用一个实验室。这些因素包括：

- 部署的复杂程度（如生产环境中的变化和计划实现的新功能）。
- 项目组的规模、位置和结构。
- 预算的规模。
- 物理空间情况。
- 测试人员的位置。
- 部署之后实验室的使用。

本章的注意事项适用于为测试 Windows 2000 Server 或 Windows 2000 Professional 设计的实验室。

将实验室用于风险管理

一个设计考究的测试实验室能提供可控制的环境，可用于整个项目期，从对技术进行试验，到比较设计方案，到调整应用过程。好的实验室不一定要投入大量资源或资金，它可以是小屋中的几个硬件，也可以是数据中心环境中的完整网络。

测试实验室是一项一次性投入可反复使用的投资，所需的由于测试较差的解决方案产生的支持和重新部署的费用很少。这是 Windows 2000 项目中风险管理规划的重要组成部分。当测试中发现下列问题时，可以明确实验室的风险：

- 硬件或软件不兼容
- 设计缺陷
- 性能问题
- 互操作性问题
- 对新技术的认识有限
- 操作或部署效率差

当测试中发现这些问题时，实验室可以提供开发和检验替代方案的手段。实验室也可用于：

- 设计和检验先前的规划，这样可以减少先导测试和生产应用期间业务风险。

- 学习如何优化部署过程，这样可以减少花在部署活动中的时间和费用。
- 制定有效的管理步骤，这样可以减少部署之后进行维护所需的时间和人员。
- 对照项目规划检验进展情况并改进项目日程安排。

实验室开发过程

图 4.1 是准备测试实验室各阶段的流程图。在制定策略阶段，确定实验室目标和大概的步骤。在本阶段所做的决定会影响设计阶段的决定。

在设计阶段，计划和记录实验室的逻辑和物理结构。在设计阶段所做的决定会影响建立阶段所建的结构。

在建立阶段，在开始 Windows 2000 测试开始之前布置实验室和测试网络组件。设计和建立阶段是相互交替的：随着认识的深入、需求的发展和测试重点的改变，需要重新设计和重新建立实验室的组件。如果在硬件、软件或测试方法中所积聚的变化开始影响测试结果，就需要重新建立组件。

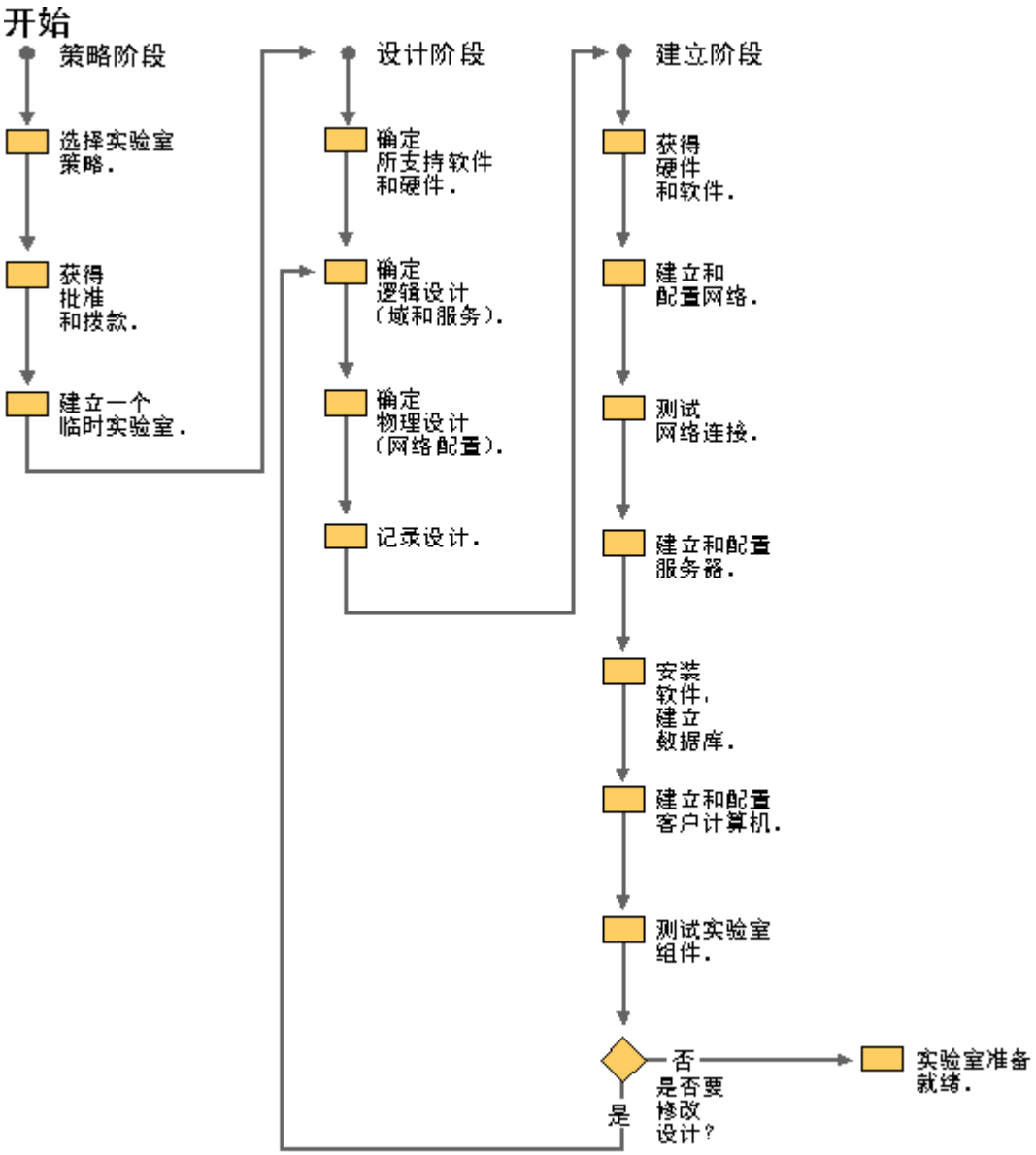


图 4.1 建立测试实验室的过程

测试过程

图 4.2 是在实验室规划和实施测试各阶段的流程图。

主要活动是：

- 制定描述范围、目标和方法的测试规划。
- 设计描述如何实施测试的测试案例。
- 实施测试和评估结果。
- 记录测试结果。
- 将暴露出的问题上报给有关人员解决。

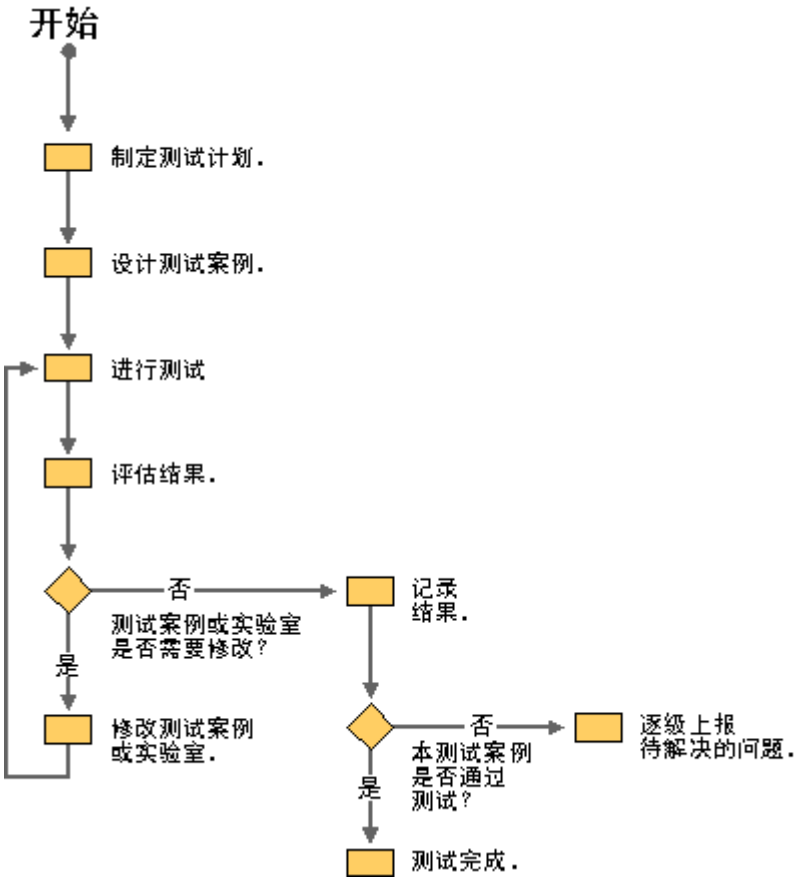


图 4.2 规划和实施测试的过程

建立初步的实验室

如果还没有实验室，那么在 Windows 2000 部署项目中尽快从实验室开始工作至关重要。在规划阶段的早期需要实验室了解有关产品、证实概念、对照业务模型测试不同的方案并检验解决方案。在项目的早期可以选择位置、开始评估硬件要求、重新配置现有实验室设备，还可能为实验室添置硬件或利用旧硬件。

如果为必要的设备提供足够的空间并为精确测试提供适当的配置的话，早期的规划在测试时将发挥作用。在决定测试的硬件、软件和人员需求时，将这些内容记录在测试规划中。有关测试规划的详细信息，参见本章稍后的“ 测试 ”一节。

如果计划建立一个长期实验室，必须获得独立于 Windows 2000 部署项目的管理层的批准和拨款。如果是这样，尽快开始审批过程。

在规划过程的早期，实验室可以帮助您建立基本名称空间设计和高级部署规划，这些东西可以用作进一步测试和发展的基准。使用实验室作为基准配置然后在各阶段中添加功能，可以避免产生与各自独立的设计相关的问题。

若要开始探索测试，可以使用两个或三个服务器和客户机建立一个临时实验室，使用现有实验室，或在办公室建立一个服务器/客户计算机配置。然后，在决定高级设计时，将这些部分集成到一起，形成正式的实验室。

尽管实验室在整个项目过程中不断发展，反映出测试重点的变化，也要确保它在先导测试前集成测试以前是装备完全的，而且是稳定的。

确定实验室策略

您也许已经有计划用于 Windows 2000 测试的实验室，也许希望为本项目新建一个实验室。无论当前是哪种情况，都应该通盘考虑实验室的目标和它的长期用途。您也许觉得现在正是将为其他目的而建的实验室升级的时候，这样将就可在 Windows 2000 环境的更改管理中发挥作用。

如果已经有一个长期实验室，计划用于测试 Windows 2000 设计，也许需要直接阅读本章稍后的“ 设计实验室 ”。

考虑投资的回报

如果决定为 Windows 2000 部署测试新建实验室，必须向项目赞助商说明投资的理由。要做到这一点，要通盘考虑所有相关的费用。在实验室中进行的测试，实现起来干净利落，支持费用也减少。使用实验室开发运营效率工具，例如自动管理工具和远程程序，可以降低本单位的总体成本。仔细审查之后，建立和维护实验室的成本很可能比将问题出在生产中、出在重新部署考虑不周或测试不彻底的解决方案中、或出在管理使用消耗大量资源的过程的生产环境中的成本要低。

在一些单位为不同的项目建立不同的实验室，规模经济也是可行的。合并几个实验室，并为新实验室的使用和维护制定一套完整的制度，可以使几个项目共用一个实验室，从而降低成本。如果决定共用一个实验室，尽量选择有比较一致的日程安排和设备要求的项目。这样，为新项目增添几个新部件来升级实验室将比每次重新购买更方便，成本更低。

实验室的用途越多，建立和运行实验室所需的空间、设备和支持的投资越合理。实验室的用途包括早期的培训到实现后的问题解决。可将实验室视为培训的最初投资。甚至还可以将它用于教育目的，如给管理层或其他团体演示功能或部署过程。

在整个项目周期内使用实验室

为证明实验室成本的合理性，要考虑在整个项目中使用实验室的多种途径。本节举几个使用实验室的例子。

规划

在早期规划中，项目组的成员可使用实验室积累经验：加深他们对技术的理解，测试假设，并发现实现中的问题和支持要求。这也是寻找优化现有运营过程的途径的好时机，如明确哪些任务可以自动执行以及哪些任务可以远程执行。

随着设计的发展，项目组成员可使用实验室来试验新技术、模型和过程，同时还可以解决业务要求。这些制作原型和模型有助于做出如何实现 Windows 2000 特点和功能决定。

开发

在开发阶段，实验室可提供可控制的环境，以便测试和评估各种问题，如下所示：

- Windows 2000 功能
- 网络基础结构兼容性
- 与其它网络操作系统的互操作性
- 硬件兼容性
- 应用程序兼容性
- 性能和容量规划
- 安装和配置文件资料
- 管理步骤和文件资料
- 生产应用（过程、脚本和文件；早期规划）
- 基线通信量模式（没有用户活动的通信量）
- 工具（Windows 2000、第三方或自定义）
- 操作效率工具

部署

在先导测试部署阶段，实验室提供运营组，例如帮助中心和操作人员，以及开始规划进行中的支持结构的地方。还可以在先导测试和生产部署阶段使用实验室将部署过程中的问题隔离、复制、分析并加以解决。

部署后

部署后，技术支持组可以使用实验室复制和解决生产环境中发现的问题。实验室还是测试修改的安全地，例如更改管理过程中的 Service Pack、补丁、新应用程序或新桌面配置。

图 4.3 说明了实验室的多种用途以及各项目阶段可能发生一些活动。时间帧是估计值，并不是实际的部署。

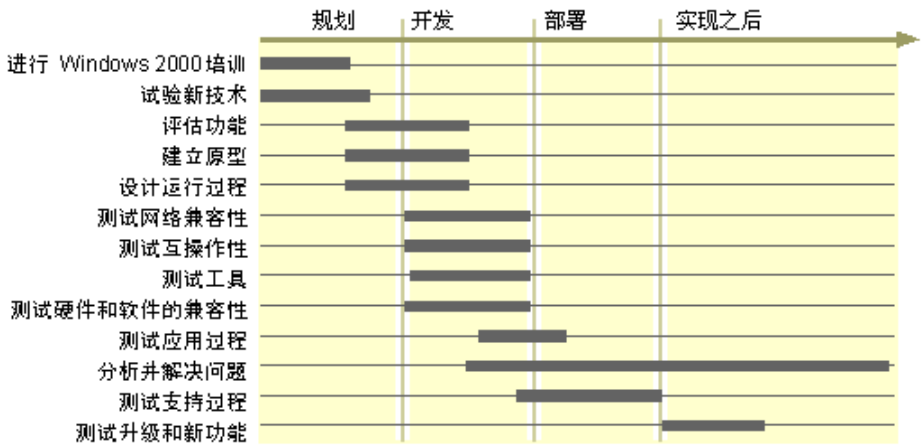


图 4.3 实验室在整个项目周期中的角色

实验室并不是进行测试的唯一地点。项目组成员还可以在单独的测试计算机上测试功能。但是，测试实验室是在模拟目标生产环境的整体环境中检验组件和功能协同工作的地方。模拟的环境应该反映中间阶段，此时功能混合，项目的后期，此时新功能已完全实现。

评估实验室模型

许多单位在每次需要为新项目测试设备时建立特别实验室。还有一些单位则为不同的项目建立一个长期的可扩展的实验室，并将它用于更改管理。更改管理实验室和特别实验室都有它们各自的优点和缺点。

特别实验室

特别实验室是为特定的项目而建立的。当项目完成以后，重新部署设备以备它用。例如，设备可用于生产环境、成为库存的一部分或者返回给供应商。

一个特别实验室的短期成本可能要比一个长期实验室少，因为所有的设备都可重新部署用于其他目的。这种关于成本的观点是缺乏远见的，因为必须为每个需要实验室的项目建立新的实验室。特别实验室可能产生下列问题：

如果每个新的项目需要新实验室，时间成为一个关键的因素。因为各个组在项目早期需要实验室，出现下列问题：

- 能否及时获得适当的硬件和软件？
- 硬件和软件替换是否会导致测试不充分？
- 能否找到要充分测试硬件和软件的产品组合所需的供应商、型号和版本？
- 能否为建立网络配置和执行测试保留必要的物理空间？
- 建立和调试实验室所花的时间是否会导致测试时间减少，从而使得测试不完全？

- 当许多组都在寻找硬件和软件许可证时，跟踪哪些人员在使用哪些设备以及谁批准了这些采购将变得相当困难。因此而引起的缺乏财务责任的行为可能导致额外的支出并增加成本。

更改管理实验室

上一节所提到的问题充分说明了建立长期的、正规的实验室的理由。在实现 Windows 2000 之后，可以用长期实验室测试环境的更改，例如：

- 网络升级
- Service pack 和软件补丁
- 业务应用程序的兼容性
- 桌面配置
- 新建硬件平台
- 管理和支持过程
- 客户计算机管理工具

用于更改管理的设备齐全的长期实验室具有下列优点：

长期使用可节约成本。

从许多项目来看，长期实验室的成本将比那些采购无法跟踪或财务责任不明确的特别实验室的成本更为合理。

降低商业风险。

实验室可降低生产环境的风险，因为扎实的测试使实现更加干净利落。例如，如果没有一个可用的测试实验室，很容易放弃对显然无关紧要的更改进行全面的测试。但是，甚至很小的更改也可能导致业务过程停止。拥有长期实验室用于更改管理使得对于哪怕是最简单的更改进行测试变得易如反掌。实验室越能真实地反映生产环境，测试的结果也就越佳。

为项目节省时间。

安装和调试的时间减到最低，因为对现有的实验室进行升级比每次重新装配新实验室快。如果计划将实验室设备用于正在开发的原型制作，节省时间是很关键的。如果使用实验室同时进行开发和测试，装配实验室的时间就会变短。

有助于适当地装备实验室。

如果计划拥有一个更改管理实验室，可能发现说明购买特殊测试所需的设备的理由更容易。在使用特别实验室时，设备很可能从其他用途调拨过来或者为满足未来使用规格而购买，而这不一定满足您的测试要求。

也许您更愿意混合使用多种设备以准确反映生产环境。随着时间的推移，可以保留原来的设备并购置新的设备以反映经常变化的、不同的生产环境。在实验室中维护设备的正确混合将在更改管理过程中保证彻底的回归测试。

有助于建立一致的方法。

如果有一个长期实验室，可以指派专职人员对它进行维护。通过长期实验室和对实验室进行连续管理，可以建立一致的测试过程和技术，这些技术可产生一致的结果，这些结果可以在不同的时间进行比较。

选择实验室模型

许多因素影响选择实验室类型的决定：特别或更改管理。下列因素可影响所做出的决定：

- 预算
- 可用于建立实验室的时间和人员
- 现有的实验室
- 物理空间或环境的限制
- 企业文化
- 项目或企业目标

做出决定的第一步是评估长期测试和风险管理目标。然后考虑与目标相关的每种模型的优点和缺点。

您可能觉得一种模型最适合您的目标，但是环境却迫使您选择另一种方法。例如，您可能看到维持长期实验室的优点，因为长期实验室可用于测试软件补丁和升级，但是您的单位却没有建立和维护长期实验室的资金。尽管需要斟酌各种方案的可能结果，这样可能想出创造性的方法以支持理想的解决方案。问问自己下列问题：

- 决定对测试质量有何影响？
- 决定对组培训和设计支持有何影响？
- 实验室是否将有助于其他现有的项目？
- 其他项目是否可以投入人力和资金共用实验室？
- 是否可以分阶段建立实验室，从最基本的组件开始然后在预算允许的范围内逐步添加？
- 硬件供应商是否同意特殊的安排？

  例如，供应商是否可以在采购之前赊帐提供设备，或提供设备，反过来将您的单位的名称用于市场目的？

选择实验室位置

有关实验室模型和实验室位置的决定很可能是互相关联的。许多团体使用的长期实验室的位置所考虑的因素要比几个团体使用的短期实验室多。例如，在规划长期实验室时，具有空间以适应未来增长的需要是一个重要问题。为了帮助您做出决定，考虑下列问题：

- 已有哪些实验室设备？它们是否正常工作？将它们改装以适合测试要求的难度有多大？
- 可否合并现有的实验室？
- 实现的规模和复杂性如何？

  如何分配实验室预算？考虑下列方面：

  - 设备和工作区费用（场地、暖气、通风、空调、电源、电缆、接插板、服务器架和工作台）。
  - 硬件和软件。
  - 维护和其他实验室人员。

- 实验室是否需要连接到生产网络或其他实验室？如果需要连接到生产网络，如何调整连接并配置路由器以保护生产网络？

有关连接实验室与生产网络的详细信息，请参见本章的“ 模拟所计划的服务器环境 ”。

选择实验室位置要考虑的其他问题包括：

升级或建立一个新的实验室

如果决定使用现有实验室，可能只需做较少的升级便能满足 Windows 2000 测试。例如，可能要将服务器升级到具有与计划部署的服务器相同的内存和硬盘容量、相同的处理器类型和速度。

开放程度

实验室应对所有想使用实验室的组开放。如果执行一种规定，项目组以外的人员来测试他们自己的应用程序，实验室应该有停车场一类的设施，接纳来访者。

安全性

确保可以从物理上保护实验室的安全，使得未经授权人员不能使用设备。

空间

无论是建立新的实验室还是将现有的实验室升级，空间都是主要的考虑事项。Windows 2000 本身并不要求具有复杂的、昂贵的设备才能开始启动和运行。因为尽可能真实地模拟生产环境很重要，所以该环境的复杂性影响实验室的复杂性。

可以决定实验室复杂性，因而也决定空间要求的现有的和建议的生产环境中的因素包括下列：

- 计划实现的功能和特点的数量和组合。

  是否计划实现跨越多个站点的域？是否计划实现虚拟专用网络 (VPN)？

- 生产环境中可变性程度。

  在生产环境中是否已有和规划部署标准设备、应用程序和配置？或是否将使用许多供应商产品、型号、版本和配置？

- 网络配置中的复杂程度。

  在生产网络中是否有多种类型的拓扑？是否计划在 Windows 2000 Server 和大型机、Macintosh 或 UNIX 系统之间建立接口？

除了生产环境中的因素，一些测试情况也可能影响实验室的复杂性。例如，可能需要附加的服务器，这样就可以如本章后面所述，将某些类型的测试分开。

空间的要求也受到可能参与测试的人数的影响。考虑要同时容纳的用户的数量。

环境条件

实验室位置应该提供适当的环境条件，例如温度、湿度和清洁的环境。这些要求类似于数据中心的要求。实验室位置也应该满足电源、电缆和网络连接的要求。

位置的数量

在某些情况下，可能要使实验室具有多个互相连接的位置，这样就可以测试在地理上分开的网络段的效果。例如，如果计划在多个 Active Directory 站点实现 Microsoft® Active

Directory™ 目录服务，可能要通过一个类似的 WAN 或 Internet 连接来测试复制。有关 Active Directory 站点和复制的详细信息，参见本书的“设计 Active Directory 结构”。

在其他情况下，可能需要多个独立的用于不同用途的实验室。可能需要一个单独的实验室用于应用程序测试或者几个不同的实验室用于 Windows 2000 Server 和 Windows 2000 Professional 的测试。

在分布式实验室环境中测试

一个实验室环境可以分布在众多的物理上甚至地理上不同的位置。下面的案例研究描述了两个单位如何决定以下面的方式使用实验室。

案例研究 1：功能实验室站点

一个大型高科技硬件厂商按产品功能生产线组织而成。它的地区办公室位于不同的地理位置，这样比较接近每个地区满足特别需要的供应商和经销商。这个制造商开发了一个跨越美国三个主要地点的实验室，从西南各州到西部各州。每个实验室的位置都是针对测试用于站点的业务的功能和配置进行设计的。每个实验室都是用于生产环境的更改管理的长期实验室。

最后该公司规划将实验室扩展以包括海外，例如远东、中东、东欧和不列颠群岛的各个城市。该单位将使用这些远程站点来设计和测试为迎接成为一个跨国企业面临的挑战的解决方案，例如：

- 在可控制的国家连接
- 慢链接
- 间断的链接
- 多种语言
- 多个时区
- 国际货币
- 计算机和网络硬件有变化

案例研究 2：偶然实验室站点

另一个单位发现在出现灾难时有所准备是很重要的。这个单位要求它的在地理上分开的站点在必要时能起到集中的信息技术（IT）部门所起的作用。在这个单位中，实验室是长期的更改管理实验室，也用于灾难恢复测试。

在发生灾难时，所选择的位置的生产机器将用于执行 IT 部门的功能。为处于准备状态，该单位在实验室执行测试以确保在备用位置所有必要的硬件和软件组件都可以使用，并可以正常工作。这些测试包括下列内容：

- 加载应用程序和数据库
- 设置配置
- 运行应用程序

设计实验室

在设计实验室之前，必须有一个高级部署规划。例如，可能需要知道计划的名称空间设计。还需要知道域结构和如何配置服务器服务，如域名系统 (DNS)、动态主机配置协议 (DHCP) 和 Windows Internet 命名服务 (WINS)。要确保实验室设计反映测试要求，项目的各个分组必须提供关于他们所需的硬件、软件和配置的信息。

如果决定建立在部署了 Windows 2000 之后可以用于更改管理的长期实验室，设计必须在空间和布局方面都足够灵活，以适应未来的需要。

设计实验室的规划越仔细，测试就越能准确地反映实际的实现的情况。

设计实验室的先决条件

因为实验室要模拟部署 Windows 2000 的环境，所以在设计实验室之前需要关于当前的和所规划的环境的信息。Microsoft® Systems Management Server (SMS) 可用于收集当前系统的信息。有关使用 SMS 盘点系统的详细信息，参见本书的“使用 Systems Management Server 分析网络基础结构”。在项目组制作的规划文件中应该有有关规划环境的信息。除了对 Windows 2000 特性和功能的深入理解之外，还需要下列信息：

- 当前的网络设计（逻辑的和物理的）。
- 规划的 Windows 2000 设计。
- 待评估和探索的功能列表。
- 现有的硬件的清单（服务器、客户计算机和便携式计算机）。
- 计划用于 Windows 2000 的硬件列表。
- 这个列表可能在测试期间有所扩充，但需要一个最初始列表来装备实验室。
- 管理工具的列表（Windows 2000、第三方和自定义工具）。
- 需要安装以用于 Windows 2000 的升级的列表，例如 Service pack、驱动程序、基本输入输出系统 (BIOS) 等。

设计测试方案

尽量将实验室设计得足够灵活。另外，至少要尽量满足下列两个标准：

- 模拟所规划的环境—设计要测试的内容。
- 适应设计过程—设计如何进行测试。

尽管您可能决定将同一实验室用于服务器和客户计算机测试，本节分别介绍实验室设计注意事项。

模拟所计划的服务器环境

计划测试尽可能多的所计划的逻辑和物理生产环境，包括计算机硬件、网络拓扑、WAN 连接、域结构、服务、数据库、业务应用程序、管理工具、安全模式、应用程序部署方法和网络服务器存储方法。

本节介绍设计实验室测试 Windows 2000 Server 需要考虑的事项。这里介绍的问题可能并不适用于所有的 Windows 2000 Server 实现。注意那些适用于您的设计的相关事项。

服务器硬件和驱动程序

在生产环境中的服务器上使用您正在使用或计划使用的相同类型的硬件组件和驱动程序。确保获得与 Windows 2000 兼容的已更新的 BIOS。

服务和配置

使用将在实际部署中使用的相同的服务和配置。例如，复制 DNS、DHCP 和 WINS 配置。如果并未打算使用 Windows 2000 中的 DNS 和 DHCP 服务，包括计划使用的第三方服务。

用户帐户

如果从 Microsoft® Windows NT® 4.0 迁移，使用生产用户帐户的副本设置域控制器作为生产域控制器的复制品。可以使用 ClonePrincipal 工具将生产用户复制到测试域。有关迁移用户帐户的策略和使用工具的详细信息，参见本书的“确定域迁移策略”。每次将生产数据复制到实验室数据库时，与 IT 安全部门协调。

域结构

如果实现 Active Directory，模拟域层次结构。例如，适当包括具有多个目录树的目录林，每个目录树中有父域和子域，以及传递和单向信任关系。在部门中反映 IT 集中和分散管理。适当地包括 Active Directory 站点。

服务器策略

包括文件和打印服务器、应用程序服务器、Web 服务器、数据库服务器和其他已在或将在生产环境中的工具服务器。如果计划使用 SMS 来部署 Windows 2000 Server，在实验室中应包括 SMS。

混合环境

要适应在阶段首次展示和完成首次展示之后的 Windows 2000 环境期间的混合环境，规划下列类型的一些域：

- 本机模式
- 混合模式
- 当前的生产操作系统

通过模拟中间状态，可以确定可能在分阶段实现期间发生的功能问题。操作系统不是 Windows 2000 Server 的服务器应该镜射当前的生产环境中的服务。

客户计算机配置

使用与生产环境中相同的客户计算机的组合。如果计划部署 Windows 2000 Server 后再部署 Windows 2000 Professional，包括部署 Windows 2000 Professional 之前一直使用的客户计算机操作系统。

如果计划首先部署 Windows 2000 Professional，测试当部署基础结构时如何将扩展服务器功能引入环境中。

如果计划有一个阶段应用，包括应用时将出现的相同组合。例如，安装了 Microsoft Windows 95 的客户计算机和安装了 Windows 2000 Professional 的客户计算机。

网络拓扑和协议

尽可能真实地镜射在生产环境中使用的网络拓扑和协议。例如，如果生产网络同时使用以太网和令牌环，实验室应该包括这两者。

WAN 连接

如果有 WAN，实验室应该有路由器以测试网络延迟时间。如果有设备和预算，可能要在远程位置建立辅助实验室以测试通过 WAN 链接的网络延迟时间。例如，应该测试通过链接的域控制器和全局编录复制。如果是一个跨国企业，建议将辅助实验室建在全世界不同的地区以测试全世界的延迟时间问题。

如果没有可用于测试 WAN 链接的辅助实验室，可以将同一实验室的两个路由器用电缆连接起来并用链接模拟器来测试链接。

远程连接

提供相同类型的远程连接，例如路由和远程访问服务以及 VPN，通过它们可以测试点对点隧道协议 (PPTP)、Internet 协议安全 (IPSec)、第 2 层隧道协议 (L2TP) 和请求拨号路由。

外围设备

包括在生产环境中使用的有代表性的外围设备的类型。例如，包括相同类型的打印机和扫描仪以及它们的相关驱动程序。

互操作性

如果计划实现 Windows 2000 Server 以操作使用其他操作系统的网络或计算机，模拟互操作性基础结构。例如，包括到大型机主机、UNIX 系统或其他网络操作系统的连接。为使实验室配置和测试套件易于管理，明确哪些互操作性方案对于本单位是最重要的，并将注意力集中于此。

管理工具

包括当前使用或计划用于基于服务器的管理任务的工具（Windows 2000、第三方或自定义工具）。必须测试工具在新的环境中的兼容性和有效性。

容错技术

测试计划在生产环境中使用的容错技术。例如，如果计划使用群集，在实验室中应包括群集服务器。

终端服务

如果计划实现终端服务，应在服务器上安装适当的应用程序。必须理解在多用户环境中运行多个应用程序的影响。可能还要修改某些应用程序的默认操作环境以获得所期望的功能。有关终端服务的详细信息，参见本书的“ 部署终端服务 ”。

注意 如果担心有一些关键的应用程序与 Windows 2000 Professional 不兼容，考虑安装终端服务。可以在 Windows NT 4.0 Server 上安装终端服务并安装 Windows 2000 客户计算机以从服务器上访问那些出现问题的应用程序。将这个方法作为意外事故计划以避免最后的安排上的疏漏。

生产网络连接

必须将测试实验室与企业网络分开。如果需要提供从实验室到企业网络的连接，计划好调节和控制连接的方法并设计出快速终止连接的方法。

设计路由器配置以保护生产网络。例如，考虑使用带有两个网卡的多宿主路由器将实验室连接到生产网络以用于特殊的、可控制的用途。配置路由器以使生产网络可以访问测试网络，但测试网络不能访问生产网络。这个方法可保护生产环境免受来自实验室的干扰，同时允许生产中的用户访问实验室的资源。例如，可以使用这个方法在将脚本移动到生产环境中的先导测试之前用较少的用户测试实验室服务器上的登录脚本。

模拟所计划的客户计算机环境

设计客户计算机实验室以便测试在生产环境中使用的相同的功能和特性。包括相同类型的硬件、应用程序和网络配置。本节介绍设计实验室以测试 Windows 2000 Professional 时需要考虑的事项。这里介绍的问题可能并不适用所有的 Windows 2000 Professional 实现。注意那些适用于您的设计的相关事项。

客户计算机硬件

至少要包括生产环境中要运行 Windows 2000 的每个供应商产品和型号包的一台客户计算机。如果单位使用膝上型电脑、插接站或端口复制器，确保包括那些供应商产品和型号。要确保准备与 Windows 2000 兼容的已更新的 BIOS。

建议为 Windows 2000 Professional 开发一个标准的硬件配置做为部署项目的一部分。实验室测试可以帮助您定义和改进标准配置。定义硬件配置时，要检验组件是否与 Windows 2000 兼容。例如，必须检验下列组件的兼容性：

- 通用串行总线 (USB) 适配器
- 光驱 和 DVD 驱动器
- 声卡
- 网卡
- 视频卡
- 小型计算机系统接口 (SCSI) 适配器
- 海量存储控制器
- 可移动存储设备
- 指针设备（鼠标、跟踪球、输入板）
- 键盘

为判断兼容性，可在 Microsoft 硬件兼容列表 (HCL) 中查找组件兼容，这可以在 http://www.microsoft.com 中使用关键字“ HCL. ”搜索到。HCL 包括 Microsoft 支持的所有硬件。如果您的硬件不在列表中，与供应商联系以查明是否有驱动程序。如果组件使用 16 位的驱动程序，必须获得 32 位的驱动程序。

也可以使用 Windows 2000 Professional 安装程序来检查硬件的兼容性。使用只检查升级的模式运行安装程序，以获得日志文件，这些日志文件中有硬件和软件不兼容以及需要更新的设备驱动程序的记录。只检查升级模式的命令行格式是：

```
winnt32 /checkupgradeonly
```

在运行 Windows 9*x* 的计算机上，日志文件是 Upgrade.txt，它位于 Windows 安装文件夹。在运行 Windows NT 的系统上，日志文件为 Winnt32.log，它位于安装文件夹。

如果设备的已更新的设备驱动程序未包括在 Windows 2000 中，与供应商联系以获得更新的驱动程序。

一旦决定标准硬件配置，检查生产环境中的计算机以确定哪些需要在部署 Windows 2000 之前升级。有关如何使用 SMS 进行盘点的详细信息，参见本书的“ 使用 Systems Management Server 分析网络结构 ”。

有关开发客户计算机标准的详细信息，参见本书的“ 定义客户管理与配置标准 ”。

网络连接

提供与生产环境中使用的相同类型的网络的连接，例如局域网 (LAN)、WAN 或 Internet。

如果计划在生产环境中使用路由和远程访问或代理网络服务，在实验室中包括这些类型的连接。

基于服务器的服务

为在生产环境中使用的服务配置服务器。例如，包括下列服务：

- DNS、WINS 和 DHCP
- 目录服务（例如 X.500 和 NetWare）
- 文件共享
- 网络打印
- 基于服务器的业务线的应用程序，包括集中的和分散的
- IntelliMirror

记住提供下列管理服务：

- 远程操作系统安装
- 基于服务器的应用程序部署
- 管理客户计算机的工具（例如 SMS）

域身份验证

如果您的单位使用或计划使用域身份验证，在实验室中模拟身份验证配置。如果从 Windows NT 4.0 迁移到 Windows 2000 Server，计划将在分阶段应用期间出现的混合环境中的身份验证。

网络管理服务

包括在环境中使用的网络服务，例如简单网络管理协议 (SNMP)。

网络协议

使用计划在生产环境中运用的协议。在将客户计算机连接到生产网络之前，首先确认在客户计算机上使用的协议。

应用程序

必须为所有应用程序获得软件许可和软件使用权，不管这些受 Windows 2000 Professional 客户计算机支持的应用程序是独立的还是基于服务器的。有关在实验室中测试应用程序的详细信息，参见本书的“ 测试应用程序与 Windows 2000 的兼容性 ”。

外围设备

包括有代表性的外围设备的类型的示例，例如在生产环境中使用的打印机和扫描仪。

服务器平台互操作性

模拟被 Windows 2000 Professional 客户计算机访问的服务器平台。如果有单独的服务器实验室，考虑将客户计算机实验室连接到服务器实验室，而不是在客户计算机实验室中安装服务器。必须建立到下列系统的连接：

- Windows 2000 Server
- Windows NT
- 支持 3270 仿真的大型机
- UNIX
- 其他的网络操作系统

如果计划在部署 Windows 2000 Server 的同时部署 Windows 2000 Professional，要包括客户计算机在部署期间可访问的任何一种服务器，除非这些测试由 Windows 2000 Server 组执行。

桌面配置

作为 Windows 2000 Professional 项目的一部分，本单位可决定评估标准客户机配置和组策略以对它们进行管理。实验室测试可以提供信息以推荐特定的配置和组策略对象进行管理。如果决定执行这种类型的评估测试，包括不同配置和组策略设置的一对一比较。

计划有足够多的相同构造和型号的计算机以便进行一对一评估。基于性能、易用程度、稳定性、硬件和软件兼容性、功能和安全模式评估客户机配置。通过验证是否产生期望的结果来评估组策略对象，特别是当多个对象应用于配置，而产生的登录时间是否可以接受。

性能

通过测试没有用户活动的基线通信量模式的变化，使用实验室开始评估对网络通信量的影响。有关性能概念和监视工具的详细信息，参见 *Microsoft® Windows® 2000 Server Resource Kit Server Operations Guide* 中的“Overview of Performance Monitoring”。

生产网络连接

客户计算机实验室和服务器实验室一样，必须与企业网络分开。如果要提供从实验室到企业网络的连接，计划好如何使用路由器将两个网络分开。

适应测试过程

因为某些测试改变实验室环境，它们可能在不注意时影响其他测试。必须注意分开、协调和管理这些类型的测试。例如，服务器升级测试会改变服务器的状态。在实验室域设计中注意这些情况。其他的情况也需要在实验室管理程序中加以注意。例如，架构变化会影响整个目录林，所以要安排好这种类型的测试并与其他的实验室用户通气。

记住实验室需要经常变化以反映当前测试重点。对基线配置进行备份，这样测试人员可以快速将计算机还原到以前的状态。确保测试还原过程。记录备份文件并将它保存到安全、方便的地点。

设计测试域

设计实验室域结构以提供一致的安装和配置，这样测试人员可以依靠状态已知的基础结构。例如，分配单个域以用于迁移和混合模式测试。
如果这样，域应总是处于混合模式状态，但专门安排的返回以前的状态以测试迁移过程的情况除外。
这样，实验室用户总能知道预期的结果。

总之，设计实验室域层次结构以将测试分到不同的域。要求不同的域的测试类型的示例为：

- DNS
- 本机模式
- 混合模式
- 迁移过程
- 生产数据的副本

设计测试域的案例研究

一个大型制造业公司设计实验室用于特殊的测试。图 4.4 是实验室的逻辑域结构。

该公司创建了一个包括四个子域的根域。域结构允许项目组为下列每一种类型的测试使用一个单独的域：

- 处于本机模式域中的 Windows 2000 Server 功能，包括打印。
- 虚拟专用网络。
- 混合模式互操作性和迁移过程。
- 与 Windows 2000 集成的 Microsoft Exchange Server。

单独的域允许小组测试 DNS 而不影响其他测试。

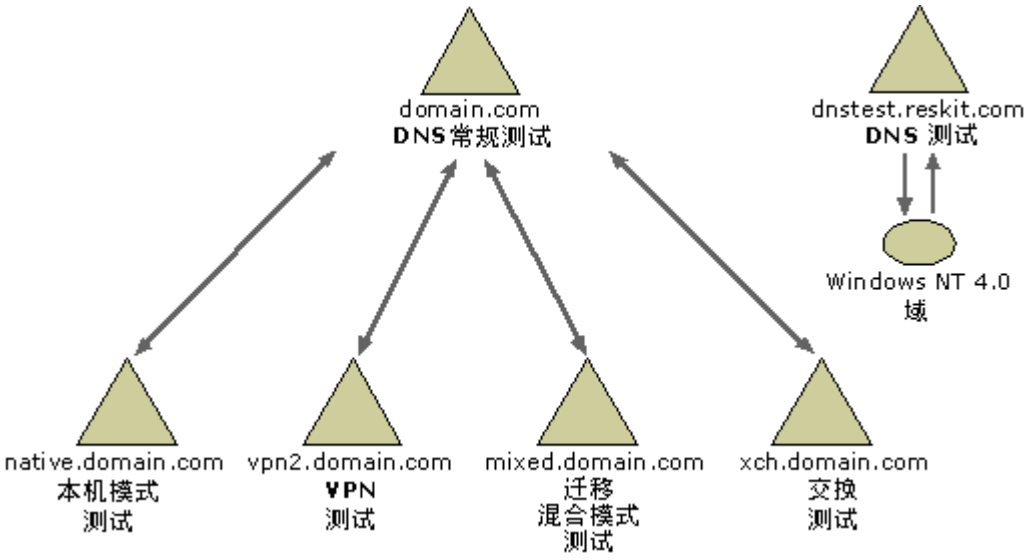


图 4.4 测试实验室逻辑域设计的示例

记录实验室配置

设计实验室时，同时使用文字说明和布局图进行记录。在实验室张贴布局图使大家很容易获得实验室信息，并让实验室使用者获得有关设计更改的最新消息。当测试人员设计测试案例以确保测试计划的全面性以及测试的可重复性时，测试人员可以使用实验室说明和布局图。

实验室说明

在实验室说明中包含下列类型的信息：

域结构，包括：

- 目录林和目录树层次结构。
- 组策略对象（设置以及它们在何处应用）。
- 每个域的目的。
- 填充用户帐户数据的方法。
- 信任关系（传递的和明确的）。

域控制器，包括：

- 如果是从 Windows NT 4.0 迁移过来的，主域控制器 (PDC) 和备份域控制器 (BDC)。
- 如果是从其他操作系统迁移过来的，提升为域控制器的服务器。

- 成员服务器，包括将在服务器上面运行的服务。

客户计算机，包括：

- 计算机构造和型号。
- 内存数量。
- 处理器类型和速度。
- 硬盘容量。
- 图形卡（类型、分辨率和色度）。

用于特定测试的实验室设计的使用，包括：

- 混合模式和本机模式测试。
- 拨号和其他远程测试。
- 互操作性测试（UNIX、主机和其他系统）。
- 复制和 Active Directory 站点测试。
- WAN 链接测试。

实验室布局图

实验室布局图应该同时显示实验室的逻辑结构和物理结构。根据实验室网络的复杂性，可以将逻辑和物理视图组合到一个布局图中。

逻辑布局图

逻辑布局图中包含下列信息：

- 域层次结构，包括目录林和目录树。
- 域名。
- Active Directory 站点。

特殊服务服务器（域控制器、全局编录、DNS、DHCP 和 WINS），具有下列信息：

- 计算机名
- 网际协议（IP）地址
- 服务器功能

- 传递信任。
- 明确的单向信任。

图 4.5 是一个逻辑布局图的示例。这个实验室有一个目录树，其中包含一个根域和三个子域。双向箭头指出 Windows 2000 域之间的传递信任。Windows NT 4.0 域与 Windows 2000 目录树有明确的单向信任关系。这个实验室没有 Active Directory 站点。在测试的这个阶段，实验室包含域控制器，其中一些是支持动态更新协议的 DNS 服务器、DHCP 服务器和一个全局编录服务器。

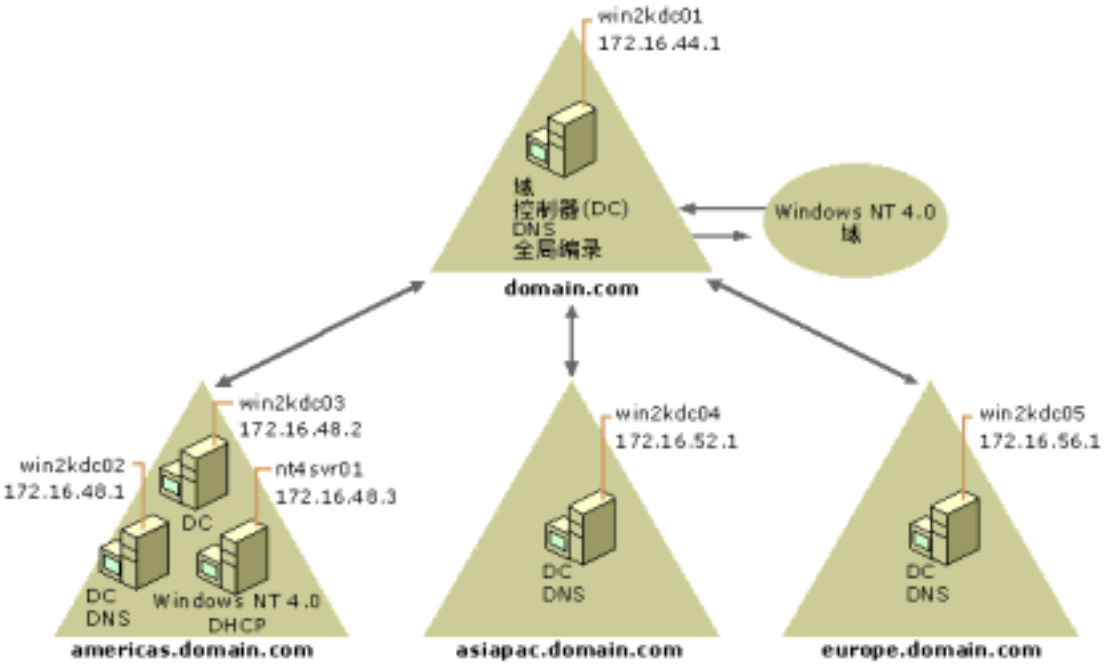


图 4.5 测试实验室逻辑布局图示例。

物理布局图

物理布局图中包含下列信息：

网络组件，例如：

- 路由器和网桥。
- 网络集线器。
- 链接模拟器。
- 代理服务器。
- 探测器和通信生成器。
- 模拟线路和 ISDN 线路。

- LAN、WAN、Internet 连接和速度。

服务器，包括：

- 域名。
- 计算机名。
- IP 地址。
- 服务器功能。

客户计算机，包括：

- 计算机名。
- IP 地址（如果使用的是静态地址）。

图 4.6 是一个物理布局图示例。这个物理布局图和图 4.5 中的逻辑布局图用于同一个实验室。在这个布局图中，可以看到三个子域的三个子网。每个子网都有一台 Windows 2000 Professional 客户计算机和另一种类型的客户计算机。实验室使用模拟的帧中继链接并有一个 UNIX 服务器。

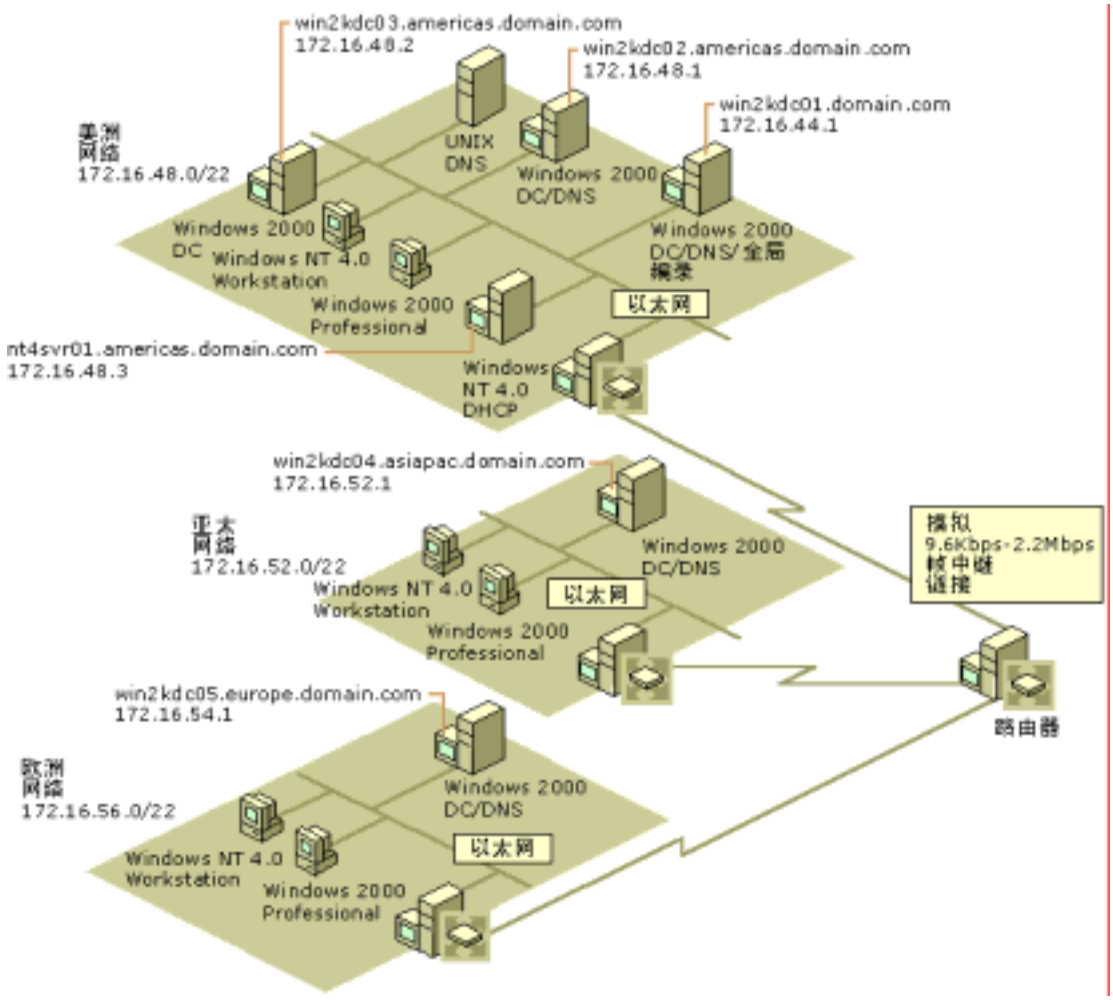


图 4.6 测试实验室物理布局图示例

建立实验室

一旦已设计和记录了实验室，让项目分组检查计划以确保已具备所有必要的条件。实验室计划获得批准之后，可以开始采购并安装硬件和软件。

如果计划随着测试重点的更改而对实验室进行定期重建，应考虑使用 SMS 一类的工具或产品对实验室的变更进行管理。同时考虑使用远程操作系统安装功能以帮助您快速更改实验室中的客户计算机配置。有关使用远程操作系统自动安装客户计算机的详细信息，请参见本书的“ 客户自动安装与升级 ”。Active Directory 服务接口 (ADSI) 和 Windows 脚本主机可帮助您快速创建、删除或更改实验室环境中的用户、组和部门。

在建立和重建实验室时，按时间顺序记录对服务器和客户计算机所做的每个更改。这个文档帮助您解决问题并理解一个特定的计算机运转的原因。也可以用来撤消最近所做的更改以解决一个短期问题。

建立实验室包括下列步骤：

- 购买硬件和软件，包括管理工具。

  可以购买或重新部署设备。所做的一切取决于预算和所选择的实验室型号。无论是哪一种情况，获得可以充分测试部署情况并反映生产设备运行情况的设备都是很重要的。

  确保所使用的硬件在 Microsoft 硬件兼容性列表 (HCL) 中。也可以联系供应商以查明产品是否适用于 Windows 2000。确保供应商为安装在硬件上的 Windows 2000 积极提供支持服务。

  使用与生产环境中将使用的硬件和软件相同的产品型号并选择相同的供应商。这个指导方针适用于：

  - 网络集线器、交换机、路由器和网桥
  - 网卡
  - 服务器硬件和操作系统
  - 客户计算机硬件和操作系统
- 安装和配置网络组件。标记所有网络线缆。
- 测试所有网络连接。

  在安装服务器之前测试网络使得发现和解决问题更容易。

- 安装和配置所有服务器。

  如果重新部署服务器，您可能需要将它们升级以适应 Windows 2000 Server。使用的内存、磁盘容量和 CPU 速度应与计划部署的内存、磁盘容量和 CPU 速度相同。一定要检查病毒并对硬盘进行碎片整理。

  安装适当的操作系统，可以是 Windows 2000 Server 或计划升级的操作系统。对硬盘分区的方法应与部署期间计划对硬盘进行分区的方法相同。

  如果正在升级域控制器，在升级之前应对服务器进行备份。测试备份并将它们存放在一个安全的地点。通过进行可靠的备份，您可以在升级步骤更改或升级失败或者需要还原到原来的状态时避免破坏生产环境。

如果购买新设备，应将组件使用两到三天以确保它们能正常工作。

- 准备好在测试中使用软件时，安装应用程序软件。安装所有基于服务器的应用程序（例如 Microsoft® BackOffice®）和生产环境中的商业应用程序。

建立或加载相关的数据库。安装您所使用的或计划使用的管理工具。

- 安装用于测试和管理的工具。如果计划验证网络流量或测试性能，您可能需要加入一个硬件探测器或软件探测器。
- 如果计划实施终端服务，应安装一套具有代表性的应用程序以便对并发用户进行测试。
- 安装和配置所有客户计算机。
- 如果计划为恢复基线配置创建备份，应设置基线配置并进行备份。

例如，如果计划从 Windows 95 升级到 Windows 2000 Professional 而不是重新安装，对装有标准应用程序的 Windows 95 客户计算机进行备份。

基线配置应该包含所有您的环境所支持的 Service Pack。确保测试并记录还原过程。

- 在实验室中测试单独组件使得与 Windows 2000 Server 和部署无关的问题分开。

当测试开始时，可能要花时间调试部署问题，而不是处理实验室的问题。

- 如果需要提供到生产网络的连接，配置和测试路由器以将实验室和生产部分隔开。

管理实验室

如果您的实验室是永久性的或被许多组使用，可能需要分配人员对它进行管理。特别是当实验室被几个组在更改管理过程期间用来进行测试时，更需要专人管理。小型实验室或由单独一个组使用的实验室可能不需要指派一个经理。即使决定不指派一个专职的经理，最好也选择一个人负责实验室。

不管是否决定需要一个实验室经理，也要建立一个良好的通信系统以发布有关实验室是否可用以及实验室状态的信息。实验室使用者需要知道他们何时可以进行测试，他们的测试是否会破坏其他测试，以及实验室所处的状态。例如，如果实验室中的一个域用于测试迁移过程和混合模式功能，实验室使用者需要了解计算机是否已准备好升级或已经升级。

如果决定安排一个实验室经理，对聘请一个专职的实验室经理和指派一个项目组成员担任此职的成本进行比较，权衡利弊。您所做的决定应取决于实验室的大小和复杂性。除了其他的项目责任以外，对实验室经理要求的额外责任可能会比较苛刻。

实验室管理责任

实验室经理必须对下列任务负责：

- 采购硬件和软件。
- 管理网络分接头以及服务器容量和配置。
- 管理硬件和软件配置以及升级。
- 协调分组之间的测试（哪些人测试哪些内容和在什么时间测试）。

如果测试要求更改服务器或客户计算机配置，这些更改必须提前计划并通知其他的实验室使用者。

- 开发和监视更改控制过程。

  更改控制过程确定出允许哪些人对实验室环境进行更改。

- 维护实验室文档（例如实验室说明、布局图和过程）。
- 建立物理安全。

  实验室经理采取措施防止对实验室设备的未经授权的使用并通过钥匙和电子锁对实验室的访问进行管理。

- 设置清单控制系统。
- 建立关于支持费用的实验室预算。
- 标记包括线缆在内的硬件。
- 解决环境问题。
- 为设备执行预防性的维护程序。
- 建立有关移除设备的批准过程（例如出借等）。
- 对服务器定期进行备份。
- 确保实验室干净整齐。

也就是说，实验室经理负责让实验室发挥最大的作用和最具灵活性。为完成这些任务而设计的所有步骤的目的都是为了便于而不是限制实验室的使用。

制定实验室指导方针

建议开发并执行一套有关小组成员应该如何使用实验室的指导方针。使这些指导方针易于记忆和遵循，尽量是阐明原则而不是下达指令。标识和记录下列各项：

角色和责任。明确谁负责诸如安排实验室的使用和执行备份一类的任务。

有关特殊类型测试的设备和指导方针。例如，标识小组成员应该用于测试迁移过程的域和配置。

更改实验室控制指导方针。明确允许何人对配置进行更改。确定更改请求的批准过程。例如，明确谁可以对计划进行更改以及更改时应该通知谁。确定当某人对实验室进行更改时所要求的文档。

服务器的初始化程序。记录安装、配置和填充域控制器和成员服务器的步骤。如果不使用 Windows 2000 内建的 DNS，应包括 DNS 设置。

测试实施的实验室还原过程。记录将域控制器还原到它们的原来状态以及刷新用户帐户数据的步骤。记录所有的服务器配置。在开始迁移测试之前测试更新过程。

客户计算机的还原过程。如果计划经常重建客户计算机以测试不同的配置，记录用来快速还原计算机到已知的初始状态的工具。例如，您可能要使用 RIS。

测试

良好的测试在您对生产环境进行更改时将减小业务风险。不过，彻底的测试要求进行认真规划。如果想要测试精确地反映出您的设计的实施情况，必须仔细设计以真实体现环境中的条件和变化。即使是一个设计良好的测试实验室也不能补偿一个设计糟糕的测试。

作为风险管理的一个关键部分，测试：

- 验证您的设计是否满足 Windows 2000 项目的业务和技术要求。
- 暴露生产环境中的潜在风险。
- 暴露项目日程安排中的潜在风险。

在规划测试时，记住对所有情况进行测试是不切实际的。不要试图测试每种组合，应把注意力集中在极限情况上。例如，测试最慢的客户计算机、最忙的服务器或者是最不可靠的网络链接。此外，集中注意那些风险最大或最有可能发生情况的区域。保持测试情况在可管理的范围内也很重要。

测试贯穿整个项目，从如下所示的组件级别（或单元）测试到集成测试：

单元测试

这些测试验证单独的功能、组件或应用程序是否适当。单元测试从设计启动时开始，持续到设计稳定时为止。对设计进行重复测试，直到提出的设计得到验证或导致修改。通常是设计人员和开发人员进行单元测试。

集成测试

这些测试验证功能和组件的协同工作状况。单元测试用于测试组件的深度，集成测试则用于测试系统的广度。

在单元测试之后、设计稳定时进行集成测试。随着设计逐渐到位，测试变得日益复杂和完整，直到它们包含了功能和组件的完全互操作性。集成测试要求一个设施齐备的测试实验室，测试人员可以在其中认真控制测试配置和条件。

建议由一个组而不是设计人员进行集成测试。许多机构都有测试组计划和实施集成测试。除了验证技术是否按计划正常实施，集成测试人员还应该从业务角度查看测试结果：他们应该考虑最终用户如何使用方案以及方案如何执行。他们也应该验证提出的方案是否满足 Windows 2000 项目的业务和技术要求。

定义逐级上报计划

在开始测试之前，确定一个出现问题时项目组使用的逐级上报计划。逐级上报计划应该处理下列问题：

- 小组成员在哪里张贴测试失败和其他结果？是否都输入事件跟踪系统或将结果输入到其他位置，例如一个 Web 站点？
- 在张贴结果或问题之前应遵循哪些步骤？例如，是否需要对问题进行复制？由谁执行？

  张贴结果时要包含哪些信息？例如：

  - 联系信息（分组领导和外部支持部门的电话号码、呼机号码和电子邮件地址）

- 问题的状态（新的或是正在进行中的）
- 问题的优先级和商业理由
- 导致问题发生的事件的顺序（包括 IP 地址和域名一类的相关信息）
- 原因（已知的或猜测的）
- 疑难解答信息（跟踪、诊断）

- 如何将这些结果或问题通知设计组？
- 谁来审查和解决这些问题？
- 通知上报的层次结构是什么？

创建测试计划

在 Windows 2000 规划的早期，每个设计分组要写一个描述他们如何测试他们的特定技术的测试计划。例如，网络组可能写一个描述他们如何测试网络功能的测试计划。在测试开始之前，分组的所有成员都应该检查和同意测试计划。测试计划中，测试案例（或状况）不断发展以描述如何测试每个特性或功能。在本章后面的“ 设计测试案例 ”部分更加详细地描述了测试案例。

测试计划适用于单元测试和集成测试。它应描述出整个测试的大致情况并应涉及到下列问题。

范围和目标

在测试计划的这一部分，描述了在测试中将包括或不包括哪些内容。例如，您可能将客户计算机硬件的测试限制为支持最少的配置或标准配置。

描述想要测试完成的任务。例如，一个机构想要从 Windows NT 4.0 环境迁移到 Windows 2000，要求一个组件一个组件地迁移，保持访问控制列表 (ACLs) 和交换权限的完整性。另一个机构要求在特定的目录服务任务中测量网络流量和观察服务器性能。

测试方法

描述将用于测试的一般策略。例如，测试计划更改的策略可能是在实验室中配置一个单独的域，这样可以更改计划而不会影响其他的实验室测试。测试计划的这一部分可能包括下列描述：

- 用于测试的域结构
- 用于实施测试或测量结果的工具和技术
- 用于测试的自动技术

需要的资源

逐条说明需要用于支持测试的下列各类资源：

硬件 例如，说明计划支持客户计算机的标准配置。包括视频卡、调制解调器和外部驱动器一类的组件。

软件 例如，包括需要测试的 Microsoft BackOffice 或其他基于服务器的产品。

数据库 包括要为测试应用程序而设置的数据库。建议将对资源的描述包括进去，例如需要填充数据库的人员和生产数据。

人员 描述所需测试人员的数量和要求的技术水平。包含顾问和其他支持人员。

培训 详细说明测试人员所需的 Windows 2000 培训以帮助他们理解正在进行测试的技术。

工具 例如，包括链接模拟器，当需要测试 WAN 链接而又没有可供使用的第二个实验室时所用。包括用于自动测试和跟踪测试结果的所有工具。

特性和功能

包含要测试的所有功能或功能的各个方面的列表。这是一个关于测试什么而不是如何测试的列表。一些机构将测试项目列表作为他们测试计划的附件。其他机构创建一个单独的文档或测试说明书，列出各项测试并简单地描述了每个测试必须包括的内容。还有一些机构将测试列表作为任务包含在他们的项目日程安排中。

下面是某个机构的测试说明书示例：

测试 1 – 信任保持

描述：当域控制器升级到 Windows 2000 时，必须保留所有到域的信任和来自域的信任。使用域目录树管理器查看信任。如果信任未出现，那么测试失败。

请注意描述并不包含对如何执行测试的说明。

在项目的后期，小组成员开发出详细步骤，描述如何执行测试计划中列出的每个测试。本章后面的“ 设计测试案例 ”部分提供了有关开发设计程序的详细信息。

测试计划应该包括下列类型的测试：

- 要执行的每个特性和服务的功能。
- 在生产环境中现有的组件和系统的互操作性，包括阶段实施期间和之后。这些测试包括阶段实施期间出现的混合环境和实施完成之后出现的 Windows 2000 环境。
- 将在 Windows 2000 上运行的每种计算机的硬件和驱动程序的兼容性。
- 将在 Windows 2000 上运行的每个应用程序的应用程序兼容性。
- 容量规划的基线和重点测试。
- 性能监视的基线。
- 配置的优化，例如客户计算机上的标准桌面。
- 部署程序和部署后管理的程序，例如对某一客户计算机进行升级并更新退出计划。
- 工具和实用程序。

关于应用程序兼容性测试的规划的详细信息，请参见本书中的“ 测试应用程序与 Windows 2000 的兼容性 ”。

风险

描述可能阻碍测试成功的已知的风险。例如，测试实验室可能比计划投入使用的时间要晚，无法获得硬件和软件，测试人员可能在做其他项目或者需要额外的培训。

日程安排

起草一个包括测试计划中列出的每个测试的日程安排。日程安排可以在使用实验室方面帮助您协调与其他分组之间的关系。

设计测试案例

测试案例是全面测试一个功能或功能的某一方面的详细程序。测试计划描述测试什么，测试案例描述如何执行一个特定的测试。需要为测试计划或测试说明中的每一个测试开发一个测试案例。

测试案例必须由理解正在进行测试的功能或技术的某人来撰写，并需要经过他人的检查。

测试案例包含下列信息：

- 测试的目的
- 特殊的硬件要求，例如一个调制解调器
- 特殊的软件要求，例如一个工具
- 特殊的设置或配置要求
- 如何执行测试的描述
- 测试的预期结果或成功标准

设计测试案例在测试日程安排中可能是时间较长的阶段。尽管您可能想走捷径，但是从长远眼光来看您在这里所花费的时间将是值得的。认真对测试进行规划可以使测试更快地得以实施。否则，测试人员将花时间调试和重新运行测试。

各个机构使用不同的方法来记录测试案例，从开发出一套详细的、类似于处方的步骤到写出概括说明。在详细的测试案例中，步骤精确地描述了如何执行测试。在描述性测试案例中，测试人员在测试的时候决定如何执行测试以及使用哪些数据。

详细的测试案例的优点是它们可以复写并且易于自动操作。当您计划在以后比较测试结果（例如优化配置）时，这个方法特别重要。详细的测试案例的缺点是需要耗费更多的时间来进行开发和维护。在另一方面，公开解释的测试案例是不可重复的，可能导致消耗更多的时间在测试本身而不是用在测试的内容上。

建议在两个极端情况之间找到一个折衷方案，这个方案倾向于吸收更多详细信息。平衡完整性和实用性以达到测试完整且易于管理的目的。

表 4.1 提供了一个详细测试案例的前几个步骤的示例：

表 4.1 测试案例示例

步骤	程序	成功标准	结果
1	注销服务器，返回到 网络登录屏幕。	无。	
2	单击域列表以打开。	本地服务器名不会出现在列表中。	
3	单击域列表以打开。	根域出现在列表中。	
4	使用具有管理特权的帐户登录到服务器。	帐户登录到服务器未出现错误。	

实施测试

在开始测试之前，如有必要先修改实验室设置以满足测试案例中指定的要求。执行测试时，仔细遵循所写的测试案例。在可以正确地评估结果或在事后复制测试以进行比较之前，必须知道测试人员执行的精确步骤。

执行测试时，根据测试案例中的标准分析结果以确定测试是通过还是失败。如果测试失败，可能是测试本身、实验室设置或提出的设计有问题。对于失败的测试，考虑以下问题：

测试案例问题。修改测试案例，重新运行测试并记录所做的所有更改。

实验室设置问题。按照实验室的更改控制过程，重新配置实验室并重新运行测试。

设计问题。按照项目的逐级上报程序通知适当的人员注意这个问题。区分各个突出的问题的优先次序并对它们进行跟踪，直到解决问题并重新测试为止。要区分问题的优先次序，考虑潜在的影响和它们出现的可能性。

记录测试结果

尽管可以在事件跟踪系统中记录问题和错误，也还需要一个跟踪系统来记录测试结果。跟踪系统可帮助您监视测试进度和测试的成功比例。该信息在管理报告、查看趋势和确认人员级别时将发挥作用。

一些机构使用基于纸张的系统，在测试案例表中记录测试结果。但是，这种基于纸张的系统使得跟踪已测试的内容和创建报告更难。

一个选择就是购买一个跟踪和报告测试案例的商业产品。另一个方法是开发一个数据库应用程序对它们进行组织和管理。通过这些方法，可以自动操作报表以监视测试结果和进度。无论选择哪种方法，项目组成员可以很容易地访问测试记录是非常重要的。有关设置测试跟踪系统的详细信息，请参见本书的“ 测试应用程序与 Windows 2000 的兼容性 ”。

无论决定使用哪种方法跟踪测试，记录每个测试的结果都是很重要的。包含下列信息：

- 测试人员的姓名和部门
- 执行测试的日期和时间
- Windows 2000 产品名（Server 或 Professional）
- 结果的完整描述
- 问题的解决
- 输入事件跟踪系统的问题编号

部署之后测试

部署了 Windows 2000 之后，如果将实验室作为更改管理过程的一部分，它将是很有用处的。不能过分强调对计算环境的更改进行测试的重要性，无论是添加新的网络结构组件、安装新的服务器、更改客户计算机的供应商、更改配置，或者是执行 Service Pack 和补丁程序。

只有一个实验室，即使是一个设计良好并且装备完善的实验室也是不够的。要发挥实验室的最大效率，确定将如何使用它以实现生产环境中的更改。记住定期评估实验室组件以确定累积更改的效果。例如，对于一台已经进行多次更改的计算机，其运行情况不同于新近安装了相同配置的另一台计算机。

将实验室用于更改管理

在将更改实际应用到生产之前，使用更改管理实验室对计划在环境中进行的更改进行测试，正如先导测试一样。当使用实验室来管理更改，它成为一个更大过程的一部分。这一过程识别出从提出更改到实现更改期间信息的流动性和活动的顺序。开发的过程取决于执行更改的类型、参与的组以及企业文化。

可以利用许多资源来帮助您将一个更改管理过程加入到 IT 环境中。第一步是先写一个更改管理计划。开始写计划之前，考虑下列问题：

- 谁授权更改？
- 如何记录和提交一个建议。
- 谁分析这些建议以确定它的重要性和影响？
- 方法和程序扮演什么角色（包括实验室）？
- 如何记录和报告更改的状态。

在实验室中测试是更改生产环境的过程中的一个步骤。许多企业在设置一个先导测试或有限的首次展示之前测试每个补丁和 Service Pack，直到被确认。在不同的状况和位置测试更改，将大大减少在执行期间遇到问题的风险。

定义实验室在更改管理中的角色

需要再次说明的是，使用实验室中的测试作为执行更改的过程的一部分是很重要的。同样重要的还有定义如何使用该过程中的实验室。可以通过描述一般更改的步骤和要求减少实验室中失败的机会。例如，明确下列内容会对您有所帮助：

- 在实验室中执行更改之前所要求的组件。
- 执行更改所要求的步骤。
- 在实验室中生成的文档。
- 如果实验室失败应采取的措施。

如果实验室成功应采取的措施。

图 4.7 表明一个重要机构如何使用其客户计算机实验室对标准桌面配置所进行的更改进行测试。

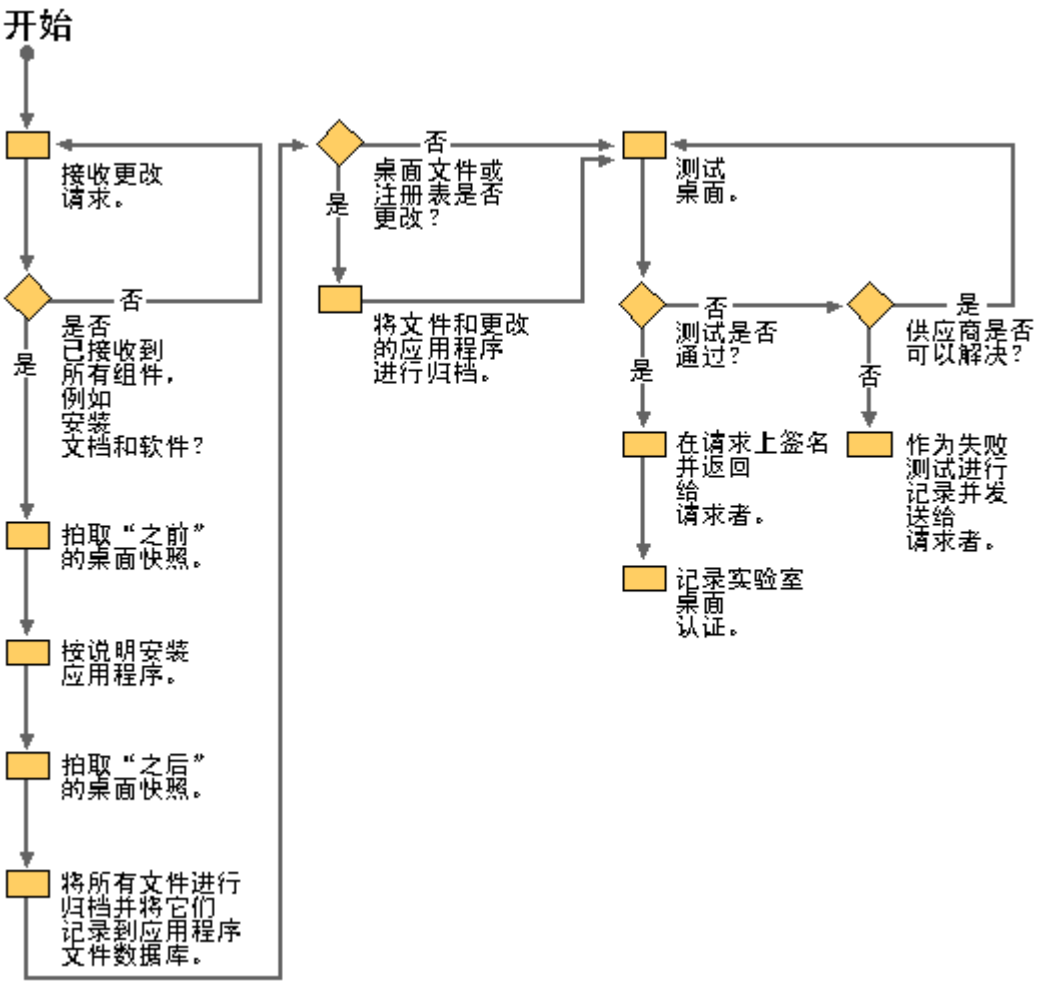


图 4.7 更改管理过程中的实验室的使用示例

实验室测试规划任务列表

使用作为快速参考的两个任务列表规划如何测试 Windows 2000 以进行部署。第一个清单用来帮助您准备实验室，第二个清单用来帮助您创建、运行和记录测试。

实验室准备任务列表

表 4.2 总结了当设计和建立一个测试实验室时需要执行的任务。

表 4.2 实验室准备任务列表

任务	所在章节
选择实验室型号。	决定实验室策略
选择一个或多个实验室。	决定实验室策略
设置一个临时实验室（如有必要）。	设置一个初步的实验室
确定实验室空间和环境要求。	设计实验室
确定电源和网络连接要求。	设计实验室
设计和记录实验室的逻辑和物理配置。	设计实验室
确定硬件要求。	设计实验室
确定软件要求，包括商业应用程序和工	设计实验室

具。	
确定谁需要使用实验室。	设计实验室
确定数据库要求。	设计实验室
确定布线和网络分接头计划。	设计实验室
采购硬件包括线缆和软件。	建立实验室
采购工作区设备，例如桌椅、白板、公告板、灯、电话和橱柜等。	建立实验室
建立和配置网络。	建立实验室
测试网络连接。	建立实验室
建立和配置服务器。	建立实验室
安装应用程序并在服务器上建立数据库。	建立实验室
安装测试和管理工具。	建立实验室
建立和配置客户计算机。	建立实验室
在客户计算机上安装应用程序。	建立实验室
测试所有的实验室组件。	建立实验室
指派实验室经理。	管理实验室
为实验室确定更改控制过程。	制定实验室指导方针
创建、测试和记录实验室还原过程。	制定实验室指导方针

测试任务列表

表 4.3 概述了需要执行的测试任务。

表 4.3 测试任务列表

任务	所在章节
写一份测试计划。	创建测试计划
建立测试案例。	设计测试案例
开发逐级上报程序。	定义逐级上报计划
实施测试和评估结果。	实施测试
记录测试结果。	记录测试结果

第 5 章 – 实施 Windows 2000 先导测试

先导测试是全面部署 Microsoft® Windows® 2000 前的最后一项重要步骤。在此之前，您必须完成实验室环境下的综合测试。在先导测试过程中，您将在一种可控的真实环境中对您的设计进行测试，这一环境也正是用户使用新建功能进行日常工作的环境。

先导测试前，项目经理及系统设计师需要针对先导测试的地点和方式作出规划。本章将帮助您制定一套先导测试的计划，选择测试用户和站点，并决定如何设置先导测试的环境。

本章内容

先导测试实施概述
先导测试计划的创建
先导测试的准备
先导测试的部署
先导测试的评估
实施先导测试规划任务列表

本章目标

本章将帮助您编制以下文档计划：

- 先导测试计划
- 先导测试的实施步骤

资源工具包中的相关信息

- 有关先导测试前的详细测试信息，请参见本书中的“ 建立 Windows 2000 测试实验室 ”。
- 有关 Microsoft® Windows NT® 3.51或更高版本迁移至 Windows 2000 的详细信息，请参见本书中的 “ 确定域迁移策略 ”。
- 有关服务器上 Windows 2000 自动安装的详细信息，请参见本书中“ 服务器自动安装与升级 ”。
- 有关客户机上 Windows 2000 自动安装的详细信息，请参见本书中“ 客户自动安装与升级 ”。

先导测试实施概述

在实验环境下验证完 Windows 2000 的设计之后，您需要在一个用户数量有限的生产环境中对其进行进一步测试。先导测试降低了全面部署过程中遇到问题的风险。

先导测试的主要目的是表明您的设计可以按预期的方式在生产环境下正常工作，且满足您单位的业务要求。其次，先导测试为安装小组提供了实践和改进部署过程的机会。

同时先导测试也为用户提供了就功能运作情况反馈意见的机会。您可以利用这些反馈信息来解决发现的问题或建立应急方案。也可以利用它们来帮助您确定全面部署后可能需要的服务支持等级。最后，先导测试将使您对是否要继续进行全面部署还是减缓部署的实施作出决定，以便您能解决那些可能对部署造成危害的问题。

为了降低部署过程中出现问题的风险，可以进行多次先导测试或设立多个先导测试阶段。例如，您可以为名称空间设计进行一次先导测试，为标准桌面配置和安全模型进行另一次先导测试，再为应用程序的远程部署进行一次测试。

先导测试过程

先导测试为迭代过程。您在可控环境中部署一定数量的计算机，评估测试结果，解决出现的问题，然后部署下一个先导测试直到您的设计满足全面部署的范围和质量为止。图 5.1 阐明了规划与实施先导测试的主要步骤。

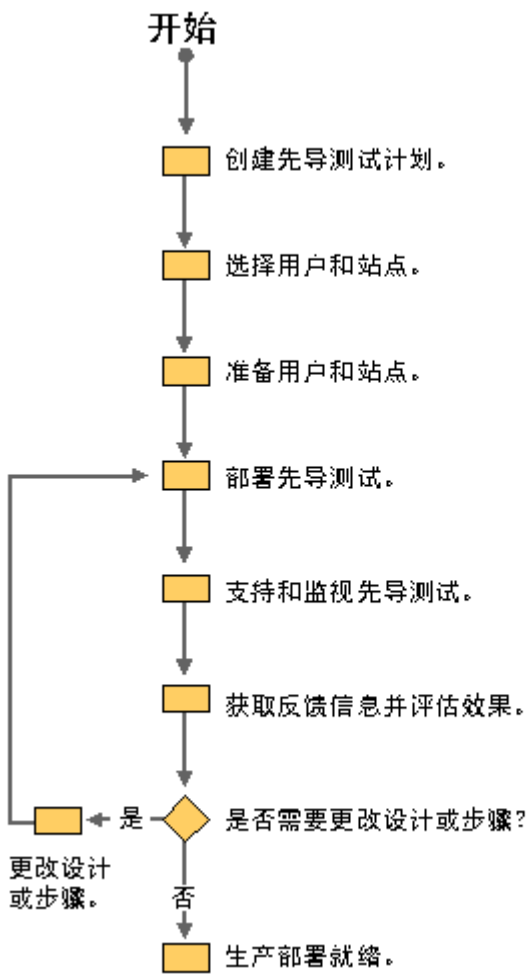


图 5.1 实施先导测试的步骤

从信息技术部门开始

如果您计划进行多次先导测试，应从小型测试着手并逐步扩大先导测试的范围。许多单位选择在其信息技术部门进行首次先导测试。他们首先建立一套模拟要在生产环境中部署的系统，参与人员使用测试网络中的测试计算机。然后这些单位再逐渐将更多 IT 人员添加到先导测试中。

在不断地将用户添加到系统的过程中，您可以利用这种 IT 先导测试解决系统的可扩展性和性能问题。在解决了所有问题之后，便可以在生产环境下开始您的首次先导测试。这时，您可以将 Windows 2000 部署于单位最终用户的生产计算机上。

生产环境中先导测试的先决条件

在生产环境下开始首次先导测试之前，实验室必须处于稳定状态，且各测试组应已完成集成和应用程序的测试。在企业网络上运行您的设计组件之前，请务必先对其进行验证。例如，验证准备使用的协议、广域网 (WAN)

链路上的复制通信流量、以及您的备份和恢复程序。您不能将任何未经实验室测试的新技术或程序引入到先导测试中。如果您实施先导测试的目标之一是测试实施过程，则安装小组应该全面彻底地开发、测试和记录这一过程。解决任何设计中尚未解决的问题或制定一项应急方案。

同时您还需要开发并验证一系列计算机升级后安装小组能运行的测试。这些测试确保安装后的系统在交付用户使用之前能正常运行。

在开始部署先导测试之前，您应就先导测试方案征得有关管理部门的许可。尽早开始您的先导测试方案以便在准备实施测试时您的交流渠道已经建立，参与者也已经准备就绪。

先导测试方案的创建

由于先导测试为全面部署设定了基调，因此您应该认真计划、与参与者有效地沟通、并对测试结果进行全面评估。为先导测试制定计划将有助于您将问题考虑透彻，并为每位参与者设定期望值。

如果存在多个先导测试，您可以制定多项测试计划。例如，每个分组均可以进行自己的先导测试，撰写自己的测试计划。测试计划应包括如下内容：

- 范围和目标
- 参与用户及地点
- 先导测试用户培训计划
- 先导测试支持计划
- 先导测试交流计划
- 已知风险和应急计划
- 复原计划
- 部署与实施先导测试的日程安排

先导测试计划准备就绪后，应将其交给 IT 管理部门和参与测试单位的管理部门审阅，在征得他们的同意后再继续您的测试计划。

范围和目标

制定先导测试计划的第一步是确定计划包含和排除的内容（范围），以及希望获得的结果（目标）。清楚地定义范围和目标有助于您设立期望值并确定成功的标准。如果可能，可以用此目标来制定先导测试方案的评估指标。您还应该为先导测试指定一个期限，既可以按时间约定，也可以按是否达到某一标准来约定。

先导测试的范围

先导测试将测试范围扩大至执行生产任务的用户。在先导测试过程中不要期望每一项功能均被测试。应将注意力集中在风险最高的功能和最有可能发生的事件上。

通过阐述先导测试包含和排除的内容对先导测试的范围进行定义。列出您计划在先导测试中包含的服务和功能以及您希望实现的目标。阐述实施先导测试可能影响的功能区域、影响的程度以及在何种情形下会造成这种影响。

列出您不准备在先导测试中包含的服务与功能。如果先导测试不能涵盖您设计中的某些方面，请作出说明。例如，如果您计划使用现有的域结构进行升级，并在以后进行重构，则首次先导测试可以不包括重构步骤。

阐述先导测试后的计划。如果您打算保留先导测试的某些功能并去除另一些功能，应在此陈述清楚。如果您认为您不想将先导测试系统作为生产系统保留下来而是要将其拆除，应事先在先导测试计划中写清退出方案。例如，如果您正在重新设计名称空间，您可以选择在先导测试后能对其进行进一步更改。先导测试计划中诸如此类的详细说明为用户事先设定了期望值。

先导测试的目标

明确陈述先导测试应该实现的目标。用这些目标作为识别先导测试成功与否的标准。多数单位拥有下列主要目标：

- 确保系统在您的环境中正常运行。
- 确保设计满足您的业务需要。
- 让用户理解并支持您的 Windows 2000 项目。

多数单位还拥有下列附加目标：

- 测试部署步骤。
- 培训安装小组。
- 为全面部署创建文档。
- 培训技术支持和支持中心小组。
- 为今后的技术支持需求搜集信息。
- 培训管理队伍。
- 开发并测试最终用户的培训材料。

先导测试用户与站点

仔细选择参加先导测试的用户和站点。首先设立您的选择条件，然后选择一种候选人的筛选方法。您可以使用的方法包括面谈、发放调查问卷和征集志愿者等。

如果存在多项先导测试，您选择的用户类型可能会根据先导测试的进程而有所不同。最终，应该包含您单位的典型用户。然而，对于一项早期先导测试而言，好的用户组应该具有如下特征：

- 能够从 Windows 2000 中获得切实的利益。
- 承担日常业务中的非关键性任务。

  一旦出现问题，用户应能承受一定时间的停机或性能降级。
- 具有目标环境的代表性。

  由于您希望使用先导测试来预测一般环境下的设计和首次安装的运行情况，因此应该选择那些没有特殊要求或不需要特定运行环境的用户群或地点。
- 使用多种计算机硬件执行不同的任务。
- 热心于 Windows 2000 项目。

- 不畏惧新技术。

  对技术不存畏惧心理的用户往往对先导测试中出现的问题更有耐心，也更有可能支持新建系统。但这种类型的用户有可能接受测试中出现的应由技术人员提供支持的某些问题。应鼓励他们报告测试中遇到的每个问题，否则您会发现他们的学习曲线并不具有典型用户的特征。在规划以后的先导测试和进行全面部署时，应将用户群的这些区别所造成的影响考虑进去。

- 愿意接受培训。

值得一提的是，对技术经验不足的用户需要多加指导使其胜任角色并在先导测试中向其提供更多的技术支持服务。

根据如下标准决定先导测试的站点数目和用户数目：

- 先导测试的目的
- 进行测试的功能与特性的数目
- 技术支持队伍的规模

在选定了测试参与人员以后，从他们之中挑选一位作为您的用户联系人。应选择一位既善于沟通又与先导测试组和项目组均保持良好关系的人。在进行先导测试规划过程中应随时与您的用户联系人合作。联系人可以为您提供有关先导测试小组执行任务类型的信息并保证小组在进入角色之前准备就绪。可以采取提供奖励项目的方式来鼓励用户参与测试并提供反馈信息。例如，您可以发放奖品或要求经理对那些在测试过程中作出特殊贡献的人员给予表扬。

先导测试培训计划

先导测试前，您必须尽早决定对参与者进行培训的时间和方式。确定用于培训的人力及其他资源。例如，可以考虑雇佣外部培训员，举行自带午餐式讲座，开发一种训练培训员项目或利用多媒体技术进行广播式培训。

大多数单位发现在安装即将开始之前进行培训可以获得最佳培训效果。决定培训应该包含的内容并估计培训可能需要的时间。将培训的内容限定于用户执行其日常工作所必须了解的范围之内。记住将培训计划列入您的先导测试日程安排表中。

先导测试技术支持计划

由于您可能需要向技术支持人员提供培训，因此务必尽可能早地作出您的支持计划。技术支持计划应指出提供支持的人员、需要提供技术支持的等级以及用户报告问题的方式。

决定由谁来支持先导测试的用户：项目小组、支持中心、还是使用外部人员？如果由支持中心来提供技术支持服务，那么您准备如何培训他们？项目小组的职责是什么？如果您进行先导测试的目的之一是培训支持中心，则需要来自项目小组和支持中心双方的资源。

决定先导测试过程中您能提供支持的服务等级。例如，关键性问题是否必须在指定时间内解决？应几个小时之内必须向用户提供技术支持？

记录先导测试变更管理和故障管理的步骤。应该提出以下几点：

- 如何提出、批准、测试和执行更改请求？
- 用户在何处公布他们的问题？

  他们是否可以向现有系统报告问题？还是需要一套诸如 Web 站点这种可以供用户记录问题的新机

制？

- 您将如何审阅问题、将问题分出优先次序并解决它们？
- 您将使用何种逐级上报过程来通知有关人员？

交流

在先导测试计划中，应阐明您将采用何种方式与参与人员进行沟通以帮助他们做好测试前的准备工作以及如何实现测试期间的状态报告交换工作。包括交流的信息类型、交流对象、方式和次数。例如，阐明您将在何时、以何种方式通知用户有关先导测试的实施。有关交流策略的详细信息，请参见本书中的“ 部署规划 ”。

决定如何在先导测试过程中进行交流的同时，您应该着手建立您将使用的交流机制。例如，为需要接收特定类型信息的不同用户小组建立电子邮件分发列表。您可以在向各分发列表上的人员发送电子邮件时注明发送的信息类型。为先导测试信息交流建立机制，如 Web 站点、常见问题、步骤以及状态报告。

先导测试复原计划

先导测试计划的一个关键部分是在测试失败情况下使用的复原步骤。制定一套详细步骤来说明进行备份的时间和方式，以及如何进行回复。例如，您将使用映像复制还是增量式备份？记录备份和还原过程并进行测试。选择一个安全的地方存放备份媒体并将具体位置记入您的复原计划。

详细说明何时使用复原计划的标准。例如，可以建立一套系统将问题的严重程度进行分级并描述允许退出测试的级别。您也可以就不同类型的问题制定相应的复原计划。例如，您可以开发用于在发生普遍故障时从整个测试中退出的计划，以及另一种用于在出现孤立性问题时从指定的组件中退出的计划。您可能还需要另一步骤用于目录服务中出现严重的数据损坏时进行复原。

日程安排

先导测试计划早期任务之一是制定日程安排。包括测试的规划、用户和站点的准备、测试的部署以及先导测试过程中的测试。不要忘记为用户、技术支持人员和安装小组安排培训时间。同时为编制站点清单、硬件升级和先导测试评估留出时间。您也可以把在规划过程中所确定的开发技术支持机制和交流机制任务列入日程安排。

为建立部署阶段的日程安排，您需要知道准备升级的计算机数目和每台计算机升级所需的估计时间。确定您每天准备升级的计算机数目和升级的次序。认真考虑一天中或一周中最适合服务器和客户计算机升级的时间。是否应该在下班后对计算机进行升级以避免中断用户的使用？是否应该在工作时间内对客户机进行升级以便用户在这段时间内参加培训？将最终用户的计算机进行升级或在他们的计算机上安装 Microsoft® Windows® 2000 Professional 之前，您是否要求他们接受培训？如果要求培训，培训计划将与先导测试的部署有关。

随着先导测试计划的进行，根据您的安装经验重新评估，您可以进一步修改您的日程安排，以获得更加准确的日程安排。

先导测试的准备

随着先导测试开始日期的不断临近，您应该着手准备测试的实施，为用户和站点留出足够的准备时间。用户测试 Windows 2000 的设计时，安装小组需要开发、测试、记录和改进实施的步骤。

先导测试站点的准备

预先准备好测试站点以便安装小组可以在测试启动时开始对操作系统进行升级。您应该已经拥有一份计算机和网络组件的清单。有关整理网络设备清单的详细信息，请参见本书中的“ Windows 2000 网络结构的准备

工作”。

对测试站点使用的计算机和网络设备进行评定后决定哪些硬件需要升级。至少确定要进行哪些改动并购买所需的组件。如果可能，应提前安装并测试这些新组件。请检查如下升级类型：

- 客户计算机升级以满足最低硬件配置需求（内存、硬盘容量、处理器速率和类型以及网卡）。
- 服务器升级以达到最佳硬件配置。
- 满足设计要求的网络升级。
- 为与 Windows 2000 （硬件、应用程序、驱动程序）兼容的客户机服务器升级。

您还需要决定以下内容：

- 在站点使用的应用程序。
- 特殊安全要求。
- 特殊连通性要求。

确保您已经就兼容性对全部硬件和软件进行了测试，安装小组也为任何特殊要求做好了准备工作。

先导测试用户的准备

与先导测试小组建立早期联络非常重要。最初的接触应该打通交流渠道并设立期望值。随着先导测试开始日期的临近，应为用户提供培训、详细的部署计划和目标日期。

建立早期的交流

一旦您选定了参与测试的人员，就应与他们见面，并进行以下工作：

- 获取参与先导测试的承诺。
- 选定一位用户联系人。
- 明确责任。
- 讨论技术支持和复原计划。

参与先导测试的人员需要理解测试的需要。理解先导测试可能对他们的工作产生什么影响，以及他们的职责。讨论先导测试的持续时间、您将提供的支持等级以及他们要执行的测试项目。尽管他们将继续其日常的业务活动，您仍可能需要就某些值得注意的领域作出详细说明。解答他们在先导测试方面或其职责方面可能存在的问题。

随时与参与人员保持联络

在先导测试计划进行过程中，用户联系人可以随时将用户所关心的问题通知您，并将测试的最新进展情况告知用户。在编制支持计划时，您应与用户进行交流，让他们了解何时以及如何申请提供支持服务、如何提交问题或有关事宜。

通知用户他们将接受哪种类型的培训以及预计培训时间。有些单位仅在部署开始之前提供一到两个小时的培训。

开始部署先导测试时，您应提醒参与人员注意如下事项：

- 培训和计算机升级的目标日期。
- 计算机升级前他们应该遵循的步骤。
- 技术支持小组联系人姓名和电话号码。

实施步骤的制定

如果您进行先导测试的目的之一是测试实施情况，则安装小组必须在项目测试阶段对这些步骤进行开发、记录和测试。虽然测试实验室是纠错的良好场所，但先导测试提供了一个真实的测试场所，在这里可以对运行步骤的精确性和效率进行调整。确保自动升级所需的脚本和工具在先导测试环境中适合于计算机使用。

在给各种类型计算机制定部署 Windows 2000 的步骤时，文档的创建对于安装人员很有帮助。实施文档可以包含如下各项：

- 安装人员所需的工具和用品清单。
- 脚本及其位置列表。
- 部署前及部署期间安装人员应制作的备份。

  包括客户计算机上用户数据的备份。
- 迁移至新建域结构的步骤。

  有关迁移至新建域结构的策略和使用工具的详细信息，请参见本书中的“ 确定域迁移策略 ”。
- 执行自动和手动计算机升级的步骤。

  如果自动方法不能正常运行可以使用手动升级方法。有关自动安装过程的详细信息，请参见本书中的“ 服务器自动安装与升级 ”和“ 客户自动安装与升级 ”。
- 为了验证部署是否能够如期正常进行，安装人员准备在部署过程中和其后进行的验收测试。。
- 安装及管理人员准备执行的操作程序（重置许可、密码变更、用户数据的复原）。
- 先导测试失败后使用的复原步骤。

先导测试的部署

在部署先导测试之前，应执行一次过程预演。包括非办公时间内执行全面升级程序的时间安排、新建设置的全面测试以及最后全部退出。

在部署先导测试过程中，应记住验证您的所有备份。清楚地标明备份并将其存放于安全地方。在执行过程中应验证每一步骤。在进行过程中，记录下安装所需的时间以便能重新修正您的时间安排。在部署过程中，应安排一位享有全部安全特权的系统管理员，其中包括拥有管理邮件和数据服务器密码的权利。

请记住记录下实施过程中作出的任何修正。在测试过程中随时进行修正，并在下一次升级过程中对这些修正进行测试。识别并记录任何效率不高的步骤和方法，利用这些信息来重新修正实施步骤。

先导测试的评估

您的小组需要在先导测试的全部过程中监视进度，解决并再测试所出现的问题。在先导测试之初将问题跟踪系统就位，鼓励用户们利用它来报告问题。由于用户可能认为问题无关紧要，或是由于他们自己找到一种解决问题的方法，所以经常忽视报告问题这一步骤。但是为了确切地评估您的先导测试，您需要用户报告出现

的每一个问题。

在先导测试的最后，您需要从各种来源中收集数据来评估测试的成功与否。在先导测试过程中积累的信息越多，您最后对先导测试的评估就越精确。

先导测试的监视

您的小组应该不断地监视先导测试网络，寻找需要调整的瓶颈及堵塞区域。监视通信流量和应用程序的性能。虽然监视工具提供了很多信息，但是定期地访问测试站点也会有所帮助。经常与用户交流有助于发现那些可能会被忽视的问题。一定要经常查看问题报告，寻找问题发展的趋势。

在先导测试过程中对项目进行风险评估。比如，可以考察如下因素：

- 作用域改变
- 成本增加
- 互操作性问题
- 意外停机

获取反馈信息

先导测试结束时，应对其成功与否作出评估，并就下一步如何进行向管理人员提出建议。然后，管理部门需要对是否在先导测试结束后继续进行该项目作出决定。为了帮助您进行评估和提出建议，应对各种来源的信息进行分析。例如，可从如下渠道获取信息：

- Web 站点反馈表
- 与业务经理进行会谈
- 问题报告
- 最终用户调查报告
- IT 项目小组的观察资料

尽量获取有关设计和部署步骤的信息。评估成功与失败的项目以便修改和更正您的计划。搜集的信息可以包括：

- 培训
- 实施步骤
- 技术支持
- 交流
- 遇到的问题
- 改进建议

使用反馈信息验证所提交的设计是否满足了设计规范和业务要求。先导测试是否达到您在测试前所确定的成功标准？如果您建立了衡量成功与否的指标，衡量先导测试的结果如何？

实施先导测试规划任务列表

表 5.1 总结了在规划先导测试时您需要执行的任务。

实施先导测试规划任务列表

任务	章节中的位置
为先导测试项目创建计划，包括： • 项目范围和目标。 • 用户与站点。 • 培训、技术支持、交流和复原计划。 • 日程安排。	创建项目规划
用户和站点的准备。	先导测试的准备
实施步骤的制定。	先导测试的准备
先导测试的部署。	先导测试的部署
先导测试的技术支持和监控。	先导测试的评估
获取先导测试的反馈信息。	先导测试的评估
先导测试结果的评估。	先导测试的评估

第 6 章 - 为 Windows 2000 准备网络基础结构

在您单位中部署 Microsoft® Windows® 2000 之前，必须先做好网络的准备工作。本章将帮助网络管理员标识部署 Windows 2000 之前需要升级或修改的网络基础结构中的具体项目，如服务器、路由器和网络服务等。同时还将就如何记录当前网络基础结构展开讨论。

阅读本章之前，请回顾本书中“创建部署路线图”和“部署规划”章节。

本章内容

记录当前环境
准备网络基础结构

本章目标

本章将帮助您制订下列规划文档：

- 当前网络环境的设备清单、布局图和文档。
- 部署 Windows 2000 的基础结构规划。

资源工具包中的相关信息

- 有关 Windows 2000 TCP/IP 的详细信息，请参见 *Microsoft®Windows® 2000 Server Resource Kit TCP/IP Core Networking Guide*。
- 有关目前的网络、基础结构和协议的详细信息，请参见本书中的“确定网络连通性策略”。
- 有关创建域迁移计划的详细信息，请参见本书中的“确定域迁移策略”。

记录当前的环境

在开始 Windows 2000 网络基础结构规划之前，记录当前网络的逻辑和物理拓扑结构以及整理一份现有软硬件的完整、准确的清单是非常重要的预备步骤。

为部署 Windows 2000 做网络准备时，应该记录当前网络环境中下面几项：

- 硬件和软件
- 网络基础结构
- 文件、打印和 Web 服务器
- 业务线应用程序
- 目录服务结构
- 安全设置

Microsoft Windows NT® 网络诊断应用程序，如网络监视器，对于记录您的网络相当有用。通常，原设备制造商会为您记录设备和驱动程序的配置提供最理想的疑难解答或配置软件。

在为 Windows 2000 准备网络基础结构的同时，您需要做相当数量的计划工作。在本书前面的“创建部署路

线图 ” 中，已经定义了部署项目的范围，选定了所要部署的 Windows 2000 功能。还确定了可能影响您规划的 Windows 2000 技术依存关系并创建了一个部署项目计划。

本章将重点介绍如何为 Windows 2000 准备网络基础结构，但准备工作不能脱离本书其它章节中的规划内容。不论是准备新建网络还是将 Windows 2000 迁移至当前的网络结构上，基础结构准备中的具体任务均取决于您的域重构、服务器升级计划和对基础结构的要求。

硬件和软件清单

如果您尚未准备这份清单，应制作一份您网络中使用的服务器和客户计算机上所有软硬件的清单。记录所有路由器、打印机、调制解调器、独立磁盘冗余阵列（RAID）数组及远程访问服务 (RAS) 服务器等硬件。一定要包含基本输入输出系统 (BIOS) 设置和打印机、扫描仪和输入设备等外围设备的配置。记录驱动程序的版本及其它软件和固件信息。

软件清单应列出全部计算机中的所有应用程序和包括您系统上与应用程序有关的动态链接库的版本号码（即日期和时间戳数据）。记录任何可能已用于操作系统或应用程序的 Service Pack。通过脚本和各种第三方应用程序，您可以从使用 Windows 管理规范 (WMI) 的 Windows 和 Windows NT 网络上获取这些信息。

Systems Management Server 对于收集 Windows NT 的相关网络信息很有用，它可以产生有关您单位的软硬件和应用程序信息的详细报告。有关使用 Systems Management Server 分析网络的详细信息，请参见本书中的 “ 使用 Systems Management Server 分析网络基础结构 ” 。

记录下服务器和客户计算机的网络配置。在运行 Windows NT 的计算机上很容易获得网络设置。

为了获取 Windows NT 下网络的设置，请

1. 单击 “ **开始** ” ，鼠标指向 “ **设置** ” ，然后单击 “ **控制面板** ” 。
2. 双击 “ 网络 ” 。
3. 记录 “ **标识** ” 、 “ **服务** ” 、 “ **协议** ” 、 “ **适配器** ” 和 “ **绑定** ” 选项卡上的信息。

在每台被指派了静态网际协议（IP）地址的计算机上，打开一个命令提示窗口，运行 “ ipconfig /all ” 命令并记录下结果。第三方硬件供应商经常提供用于搜集相关硬件和配置设置细节的诊断软件和管理软件。

您可以用这些清单：

- 与硬件兼容列表（HCL）对照，确认当前的基础结构、服务器硬件、计算机的 BIOS 和软件配置与 Windows 2000 Server 兼容。有关 HCL 的详细信息，请参见 Web Resources 页的 Microsoft Windows Hardware Compatibility List 链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。
- 确定每个服务器和客户计算机的升级路径并为购置新设备草拟规范。

网络基础结构

在记录当前的网络环境时，应特别注意目前存在问题的领域。如果在部署新操作系统之前稳定您的网络，则部署和故障排除过程将容易许多，您对升级后的系统也会更有信心。建立一个测试实验室来复制问题和配置，是评估用一套指定的协议、硬件驱动程序和客户/服务器配置部署 Windows 2000 所产生的影响的好方法。有关建立测试实验室的详细信息，请参阅本书中的 “ 建立 Windows 2000 测试实验室 ” 。

在记录网络基础结构时，您即要获取基础物理结构的硬件数据，又要获取网络上所使用的协议及其配置的软

件数据。还应该记录网络的逻辑组织、名称和地址解析方法、所使用的服务与配置。记录网络站点位置和它们之间的可用网络带宽，也有助于在升级或迁移至 Windows 2000 时作出是采用推送安装还是根据需求安装的决定。有关安装、升级和迁移至 Windows 2000 操作系统的详细信息，请参见本书中的“客户自动安装与升级”和“服务器自动安装与升级”。

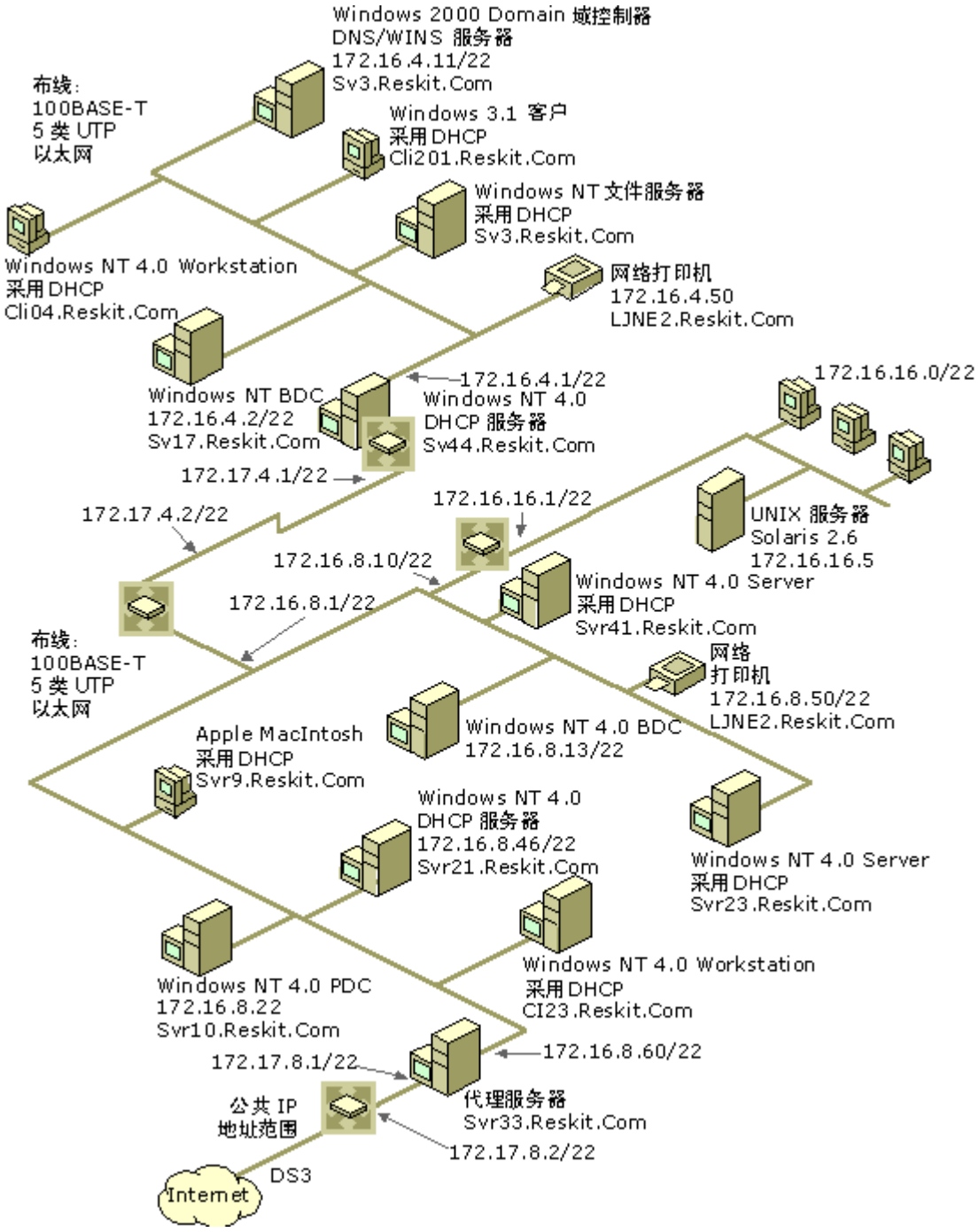
制作网络的物理和逻辑布局图有利于以一种直观易懂的方式管理您所搜集的信息。

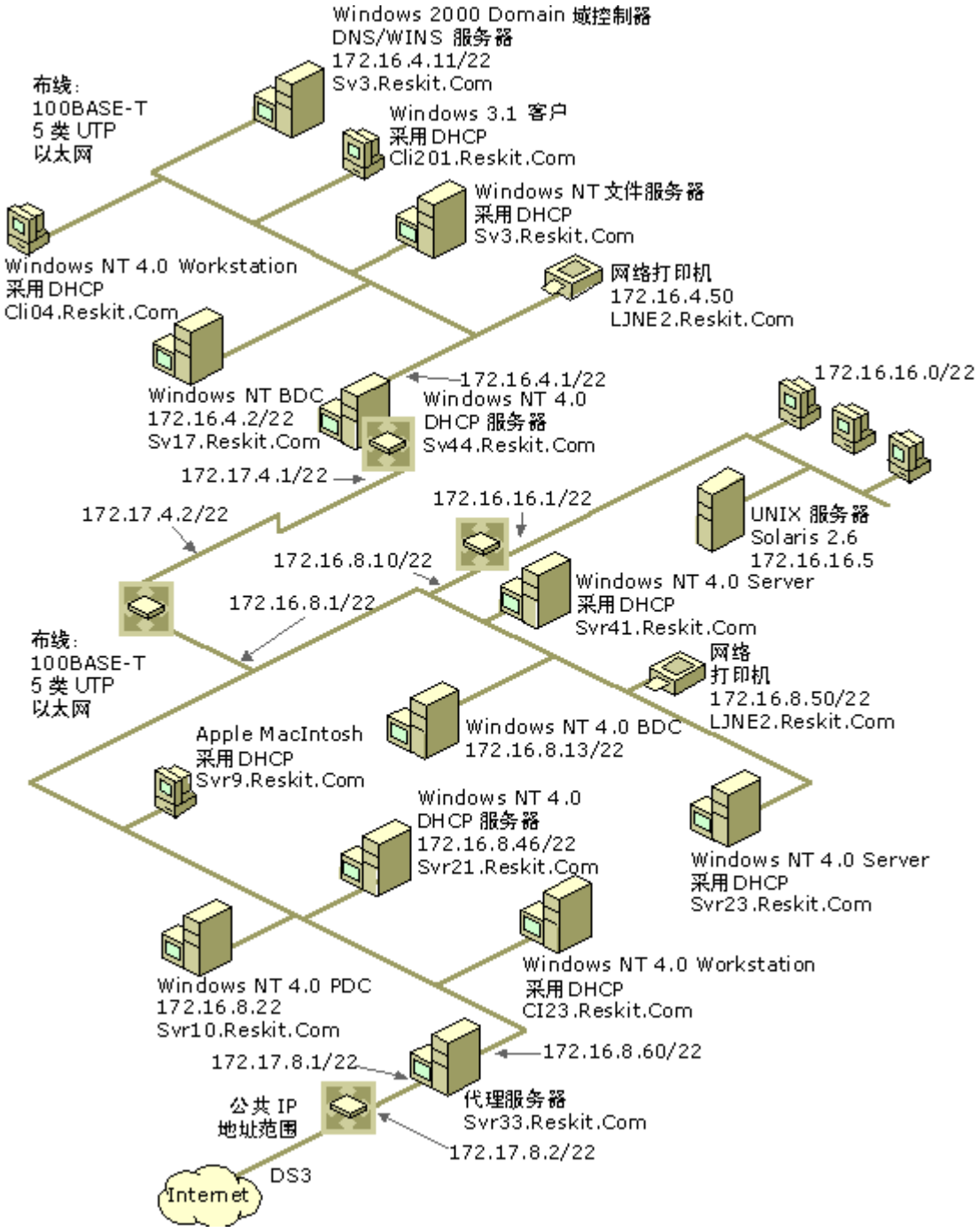
物理网络布局图

物理网络布局图标出当前网络的如下信息：

- 物理通讯链接的细节，如电缆长度、等级，物理布线、模拟和 ISDN 线路的大致路径。
- 服务器的计算机名、IP 地址（如果是静态的话）、服务器角色、域成员资格。服务器可以担任各种角色，包括主域控制器、备份域控制器，动态主机配置协议 (DHCP) 服务器、域名系统（DNS）服务器、Windows Internet 命名服务 (WINS) 服务器、打印服务器、路由器、应用程序或文件服务器。
- 网络上打印机、集线器、交换机、调制解调器、路由器、桥接器和代理服务器等设备的位置。
- 广域网 (WAN) 通讯链接（模拟和 ISDN）和站点间的可用带宽。可为估计值或是实际测量值。
- 每个站点的用户数目，包括移动用户。

图 6.1 为一个物理网络布局图示例。


Windows 2000 Domain 域控制器
DNS/WINS 服务器
172.16.4.11/22
Sv3.Reskit.Com
布线:
100BASE-T
5 类 UTP
以太网
Windows 3.1 客户
采用 DHCP
Cli201.Reskit.Com
Windows NT 文件服务器
采用 DHCP
Sv3.Reskit.Com
Windows NT 4.0 Workstation
采用 DHCP
Cli04.Reskit.Com
网络打印机
172.16.4.50
LJNE2.Reskit.Com
Windows NT BDC
172.16.4.2/22
Sv17.Reskit.Com
172.16.4.1/22
Windows NT 4.0
DHCP 服务器
Sv44.Reskit.Com
172.16.16.0/22
172.17.4.1/22
172.17.4.2/22
172.16.16.1/22
UNIX 服务器
Solaris 2.6
172.16.16.5
172.16.8.10/22
Windows NT 4.0 Server
采用 DHCP
Svr41.Reskit.Com
172.16.8.1/22
布线:
100BASE-T
5 类 UTP
以太网
网络
打印机
172.16.8.50/22
LJNE2.Reskit.Com
Apple MacIntosh
采用 DHCP
Svr9.Reskit.Com
Windows NT 4.0 BDC
172.16.8.13/22
Windows NT 4.0
DHCP 服务器
172.16.8.46/22
Svr21.Reskit.Com
Windows NT 4.0 Server
采用 DHCP
Svr23.Reskit.Com
Windows NT 4.0 Workstation
采用 DHCP
CI23.Reskit.Com
Windows NT 4.0 PDC
172.16.8.22
Svr10.Reskit.Com
172.17.8.1/22
172.16.8.60/22
公共 IP
地址范围
代理服务器
Svr33.Reskit.Com
172.17.8.2/22
DS3
Internet


Windows 2000 Domain 域控制器
DNS/WINS 服务器
172.16.4.11/22
Sv3.Reskit.Com
布线:
100BASE-T
5 类 UTP
以太网
Windows 3.1 客户
采用 DHCP
Cli201.Reskit.Com
Windows NT 文件服务器
采用 DHCP
Sv3.Reskit.Com
Windows NT 4.0 Workstation
采用 DHCP
Cli04.Reskit.Com
网络打印机
172.16.4.50
LJNE2.Reskit.Com
Windows NT BDC
172.16.4.2/22
Sv17.Reskit.Com
172.16.4.1/22
Windows NT 4.0
DHCP 服务器
Sv44.Reskit.Com
172.16.16.0/22
172.17.4.1/22
172.17.4.2/22
172.16.16.1/22
UNIX 服务器
Solaris 2.6
172.16.16.5
172.16.8.10/22
Windows NT 4.0 Server
采用 DHCP
Svr41.Reskit.Com
172.16.8.1/22
布线:
100BASE-T
5 类 UTP
以太网
网络
打印机
172.16.8.50/22
LJNE2.Reskit.Com
Apple MacIntosh
采用 DHCP
Svr9.Reskit.Com
Windows NT 4.0 BDC
172.16.8.13/22
Windows NT 4.0
DHCP 服务器
172.16.8.46/22
Svr21.Reskit.Com
Windows NT 4.0 Server
采用 DHCP
Svr23.Reskit.Com
Windows NT 4.0 Workstation
采用 DHCP
CI23.Reskit.Com
Windows NT 4.0 PDC
172.16.8.22
Svr10.Reskit.Com
172.17.8.1/22
172.16.8.60/22
公共 IP
地址范围
代理服务器
Svr33.Reskit.Com
172.17.8.2/22
DS3
Internet

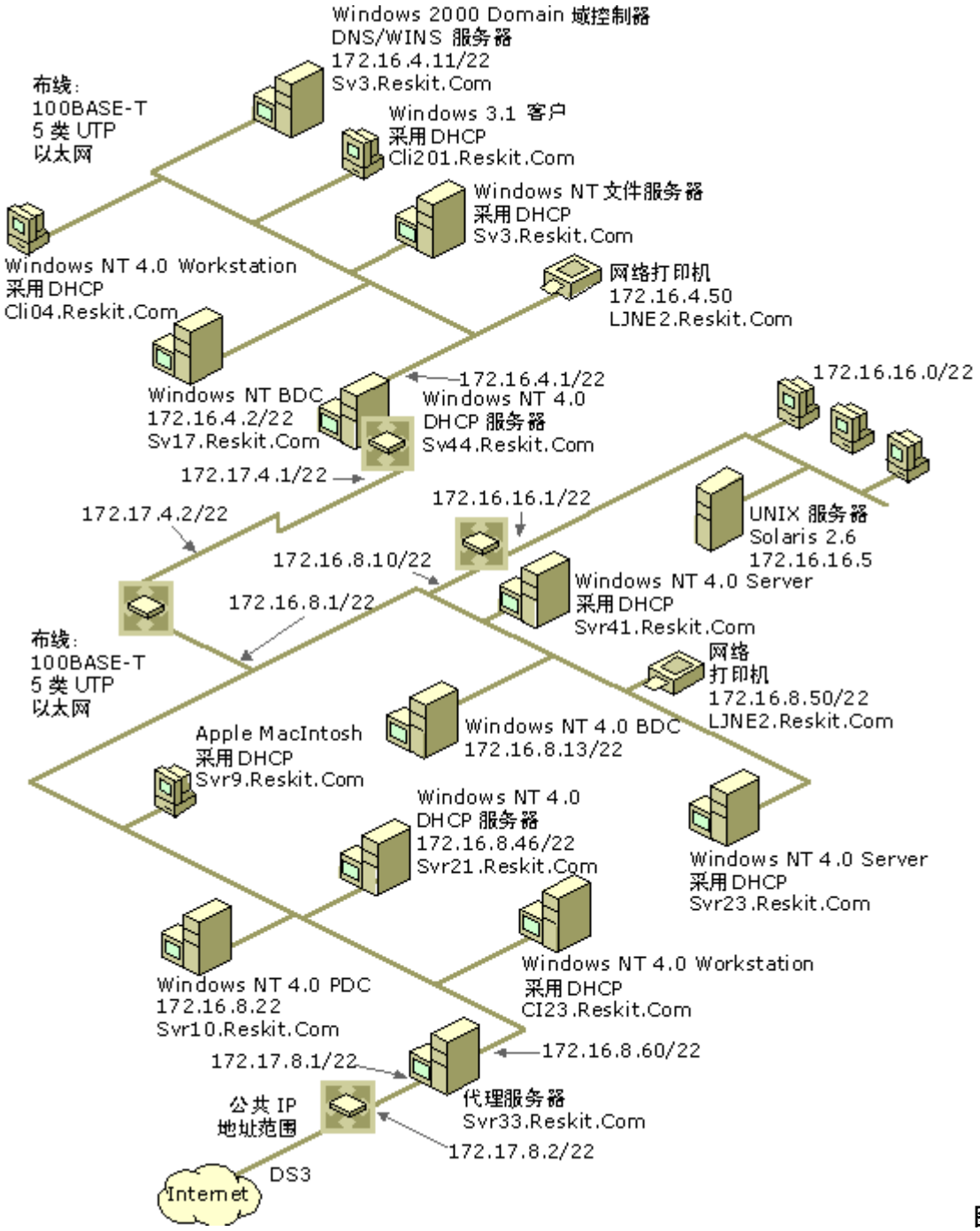


图 6.1 物理网络布局图

记录下网络上所有设备的固件版本、吞吐量和特殊配置要求。如果这些设备有静态 IP 地址，应记录下来。有关网络连通性和 Windows 2000 的详细信息，请参见本书中的“确定网络连通性策略”。

逻辑网络布局图

逻辑网络布局图展示网络的结构，包括：

- 域结构，包含现有域层次结构、名称和寻址方案。

- 服务器角色，包括主域控制器、备份域控制器、DHCP 服务器或 WINS 服务器。
- 信任关系，包含可传递、单向和双向信任关系。

图 6.2 为逻辑网络布局图示例。

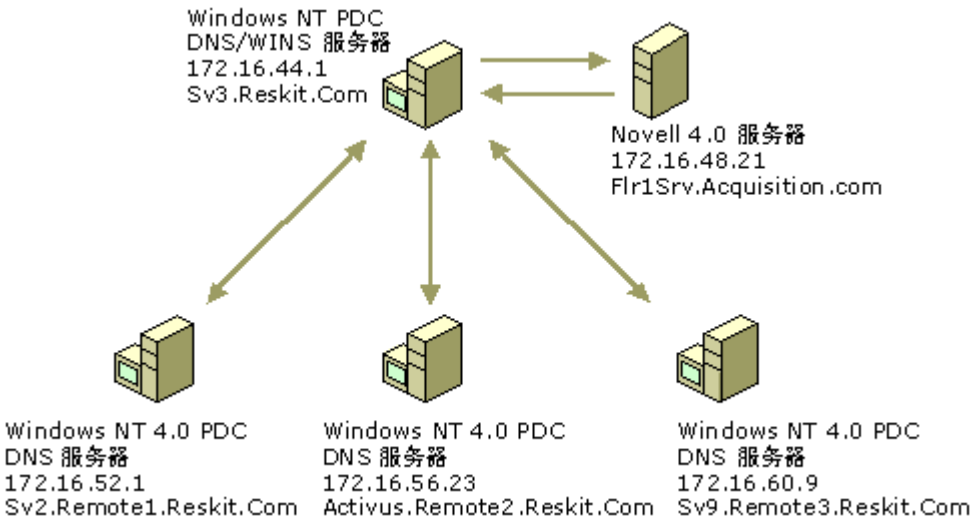


图 6.2 逻辑网络布局图

网络配置

一般情况下需要记录的网络配置内容包括下面几个部分。

名称解析服务

确认您已经记录了网络上所有的 DNS 和 WINS 服务器，记下配置和版本信息以及硬件细节。注意网络上是否存在能够支持动态注册和服务 (SRV) 资源记录而未运行 Windows NT 的 DNS 服务器，软件制造商是否提供此性能的升级。

如果网络上有不运行 Windows NT 的主机，记录它们所使用及提供的服务，如 UNIX BIND。应该记录每项服务的版本。例如，如果网络上使用了 BIND，应注意低于 4.9.4 版本的 BIND 与 Windows 2000 不兼容。如果网络上有服务广告协议 (SAP) 和路由信息协议 (RIP) 服务，请记录下来。

IP 寻址方法和服务配置

确认已经记录了网络上所有的 DHCP 服务器，包括：

- 所有已经分配给服务器或客户计算机的 IP 地址。
- DHCP 设置，如默认网关。
- 子网的细节，并将其与总体的域结构联系起来。
- 网络中子网和主机的数目，并记录 IP 地址和子掩模。
- 客户能够在网络中租用 IP 地址的期限。

远程和拨号网络

如果您拥有远程或移动用户，记录远程访问和拨号的配置。如果为移动用户使用了第三方软件，审阅并记录这些产品的配置。如果您使用了虚拟专用网络 (VPNs)，记录 VPN 的配置以便决定是否能用 Windows 2000 VPN 替代它。

带宽问题

记录网络当前带宽的使用情况。其目的是建立一个用于衡量变化的基线。有许多第三方和 Microsoft 工具都可来测量带宽状况，包括接收或发送的字节和数据包数、传送和接收错误、每秒传送的数据包等。记录单位网段和各地理区域间的网络链接速度。

从带宽的角度考虑您单位的逻辑和地理分布情况。是否拥有分支机构、移动或远程办公人员？考虑您单位通讯链接的通信数量和类型。例如，WAN 链接是否会由于不同地点域控制器间的域复制而时有减慢？记录所有 WAN 链接和网段的可用带宽。设法记录网络在低谷、正常和高峰期的可用带宽。

文件、打印和 Web 服务器

记录成员服务器的配置细节，请格外注意任何特殊的配置，如带有一组调制解调器的服务器，或有多个网卡的部门服务器。分清服务器是企业服务器还是部门服务器。留心服务器的任何特殊操作要求，标明这些服务器是否需要特殊的协议或驱动程序。例如，如果某产品需要驻留在备份域控制器，当备份域控制器升级至 Windows 2000 时，此产品的功能就会受到影响。同任何其它计算机一样，要用 HCL 评估这些计算机上的硬件和相关驱动程序与 Windows 2000 的兼容性。

确定您单位中打印机的位置并记录它们的配置。在部署规划中应特别注意代理服务器和 Web 服务器，您需要对此级别的服务器的安全影响和每个服务器能够要求的带宽多加考虑，尤其是 Active Directory™。有关文件、打印和 Web 服务器规划的详细信息，请参见本书中的“升级和安装成员服务器”。

业务线应用程序

确认所有您单位在执行核心任务时必须使用的应用程序。通常的核心应用程序会包括数据库应用程序、电子邮件系统、和财务软件包等，所有这些程序都必须准确无误地运行才能保证您单位商务活动的正常进行。检查这些应用程序是否与 Windows 2000 兼容。例如，如果希望将您的电子邮件系统与 Active Directory 进行集成，必须与您的供应商联络，查询是否有现成的或计划中的实现 Windows 2000 和 Active Directory 兼容的升级路径。为了保证产品能够在 Windows 2000 上正常运行，许多软件供应商已经与 Microsoft 结为伙伴关系。“Certified for Windows” 徽标便是兼容性的最好保证。有关应用程序是否与 Windows 2000 兼容的详细信息，请参见本书的“测试应用程序与 Windows 2000 的兼容性”。有关与 Windows 2000 兼容应用程序的详细信息，请参见 Web Resources 页的 Directory of Windows 2000 Applications 链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

目录服务结构

把记录当前域结构放进移至 Active Directory 的计划中。明确您单位的域结构、用户和用户组及其地理位置、资源和管理域。记录域间的单向和双向信任关系。记录是否拥有一个由公司收购、合并或其它操作所产生的不连续的名称空间。这些信息将在规划 Windows 2000 域目录林和确定信任关系类型时发挥作用。

明确网络上任何不属于 Windows NT 的目录服务，如 Microsoft® Exchange Server 目录服务扩展程序，或 UNIX BIND。标识所有的用户帐户。这些帐户信息将在迁移至 Active Directory 和维护 Active Directory 与其它目录服务间的正常工作中发挥作用。

域管理模型

确认域管理的主要管理模型（或标准）。您是否拥有一个集中的、具有层次结构的管理模型？您的单位是否许可分布式管理模型？与单位总管理员相比较，本地管理员能做些什么？您单位的管理模型是否有重叠部分？这些信息将帮助确定管理职责能否可以在 Windows 2000 下重新组织，以便使域管理可以更高效率、更低成本地进行。Windows 2000 在帮助您管理网络中最大型和最小型任务的能力方面具有重大改进。

在检查当前域结构时，记录网络的如下信息：

域结构的类型 大多数网络拥有多个主帐户域，以及更多的资源域。在对当前域进行迁移或升级时，现存域结构可能会影响 Windows 2000 域结构的设计。有关的详细信息，请参见本书的“确定域迁移策略”。

当前信任关系 记录网络中当前的单向和双向信任关系。标识任何不准备移至 Windows 2000 域目录林中的域与信任关系。升级至 Windows 2000 域且被指定进同一目录林的域将通过可传递信任关系与其它 Windows 2000 域连接。在将域升级到 Windows 2000 以后，需要在 Windows 2000 域与您不想移至新目录林的域之间建立显式信任关系。

网络上域控制器的数目和位置 有利于进行所有域的升级计划。您应该在物理网络布局图和逻辑网络布局图中标识出主域和备份域控制器。注意其物理位置和配置细节。有关确定域控制器升级顺序与时间的详细信息，请参见本书中的“确定域迁移策略”。

当前的 DNS 名称空间 了解您单位现有的名称空间将有助于为 Windows 2000 目录林建立一个独特的名称空间。规划中的重要一步是选定一个 DNS 名称空间作为 Active Directory 层次结构的根，因为一旦设计好层次结构就不容易更改根名称空间了。有关为 Active Directory 规划域结构的详细信息，请参见本书的“设计 Active Directory 结构”。

安全性

即使不移至一个新建的操作系统，评审您单位的安全性标准及其实施方式也会有所帮助，但如果真的迁移时，则评审将发挥更大作用。检查移动与桌面用户、内外部网络、拨号和远程访问帐户的安全性标准和步骤。

创建用户、用户组和文件共享，更改密码，配置设备和对象属性等管理任务是集中进行还是分组进行？这些小组的具体权限和成员资格是什么？

记录您单位当前办公地点、业务单位、部门之间的关系类型。这些部门的管理任务属共享管理还是独立管理？用户小组是来自单位的不同部门或地点，还是按部门组成？记录这些信息和所有当前用户与企业的安全策略。记录不同小组能够接触的信息类型，以及对某些类型的信息如财务数据的严格限制条件。

记录有关正确使用网络的指南，如有关职员是否可以访问 Web、访问的目的、什么行为构成禁止的、不恰当的访问。

您单位与外部供应商、客户、合资企业或商业伙伴的关系将影响您的安全策略。请回答如下与单位关系相关的问题：

- 是否给予您的伙伴服务级承诺？是否许可他们在认可的用户级上访问您的网络？
- 访问您网络数据和资源的策略是什么？
- 他们是否可以在只读基础上查看数据？他们能否在您网络上更改或添加数据？
- 您如何限制对应用程序的访问？

记录当前使用或今后准备使用的安全和加密标准，应包括下列信息：

- 记录网络上用户和用户组的安全许可权利。
- 列出域和域控制器间的现存信任关系。
- 记录密码标准--密码的长度、许可的字符组合、用户可以保留密码的时间等。
- 列出网络上使用的安全协议。
- 记录如何验证通过 Internet、拨号网络和广域网 (WAN) 链接到您网络的外部用户。
- 记录用户所拥有的多个帐户的细节。例如，用户是否同时拥有一个 Windows NT 的帐户和一个 UNIX 帐户？记录这些多帐户的权限、用户和用户组成员身份及其它细节。

有关创建网络安全计划问题的详细信息，请参见本书中的“规划分布式安全”。这些问题包括可能面临的安全风险类型以及设计对付这些风险的方法。作为此步骤的一部分，您将计划和开发有关公钥基础结构和用户认证的策略，和用于保护电子邮件和 Web 服务器的方法。

在审阅现存安全计划时，应审阅您的备份方案，包括是否将备份存于单位以外的地方来降低安全风险，故障恢复计划是否被更新且适合当前网络规模和要求。有关制订存储配置策略和创建灾难恢复规划的详细信息，请参见本书中的“确定 Windows 2000 存储管理策略”。

有关安全问题和计划使用 Windows 2000 的详细信息，请参见 *Microsoft Windows 2000 Server Resource Kit TCP/IP Core Networking Guide* 中的“Internet Protocol Security”，和本书中的“规划分布式安全”。

准备网络基础结构

下面各节将就如何为 Windows 2000 准备网络基础结构进行介绍。尽管每个网络各不相同，且优先级别也由许多技术和组织因素来决定，您仍可以使用图 6.3 所示的通用准备路径。

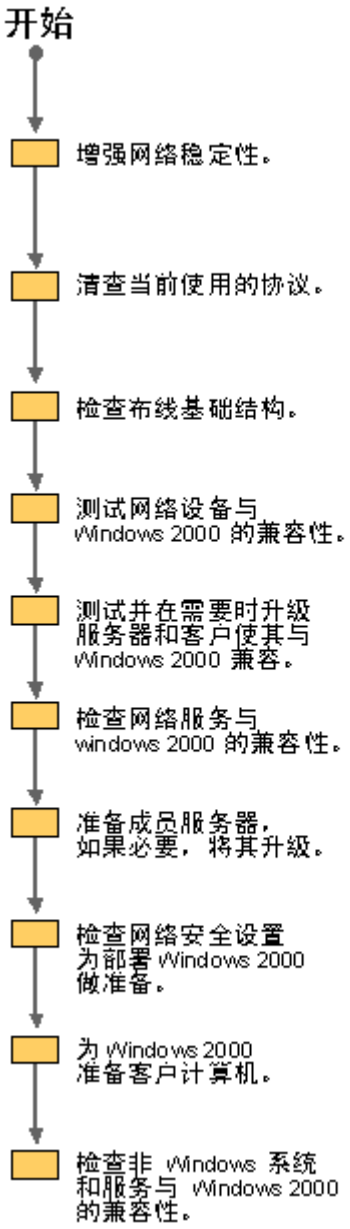


图 6.3 网络准备流程图

这些问题将分别在本书后面的章节中详细讨论。本章节介绍了在为 Windows 2000 准备网络基础结构时在这些方面应该注意的问题。同时说明了本书中哪些章节提供了有关这些问题的具体信息。

预备步骤

开始为 Windows 2000 准备网络基础结构前，应先稳定当前的系统并检查网络协议。

稳定现有网络

在实现网络升级或迁移项目之前，必须发现和消除网络传输瓶颈、更换性能不良的硬件、修改不稳定或有问题的配置，以及进行其他必要的工作。在一个迁移和升级项目中，余量不多的带宽和不稳定的网络组件将给

项目目标的实现造成困难。

将不稳定的计算机、外围设备和网络设备列入硬件升级计划。升级之前，更新网络维护时间安排表。在替换网卡等网络设备时，使用与 Windows 2000 兼容的设备进行更换，兼容设备清单列于 HCL 中。

检查网络协议

每个网络均使用各种适当的协议。根据网络、身份验证、安全需求以及所使用的操作系统性能的不同，维护以太网的机构有可能使用 TCP/IP、NetBEUI、SPX/IPX 和其它协议的组合。 标识您网络所用的协议。标识过程中，考虑这些协议是否可以用 Windows 2000 版本来替代或由于不再被已经升级的客户所需要而完全删除。例如，如果在迁移中所有 IPX/SPX 的客户都被 Windows 98 或 Windows 2000 Professional 客户所替代，您就可以在网络中删除 IPX/SPX 以释放带宽。应考虑只使用 TCP/IP 协议组来简化您的网络。

Windows 2000 推出的 TCP/IP 协议组提供了比以前更多的功能，如大窗口支持和选择性认可功能。您须使用 Microsoft TCP/IP 协议栈才能使用如 Active Directory 支持等特定的功能和利用 Windows 2000 的高级功能。例如，旧版本 Windows NT 使用点对点隧道协议 (PPTP) 来保证通讯链接的安全。Windows 2000 支持 PPTP，但也支持第二层隧道协议 (L2TP)，因此可提供增强的性能与通讯链接的安全性。有关 Windows 2000 TCP/IP 协议组功能和性能增强的详细信息，请参见 *Microsoft Windows 2000 Server Resource Kit TCP/IP Core Networking Guide* 中的“ Windows 2000 TCP/IP ”。

准备物理基础结构

考虑当前网络布线和设备的质量和带宽是否能支持升级或迁移计划。集线器、电缆等网络设备是否满足速度要求？链接到不同地域站点的速度有多快？网络内部和链接上的通信流量的大小？例如，只使用文字处理软件或电子制表软件作为其主要桌面应用程序的远程机构并不给分支服务器产生太大的通信流量，因此能达到 10-Mbps 传输速度的 3 类 网络布线与拥有同样速度的集线器可能就满足要求。在总部，共享数据的共享应用程序如：数据库和财务系统是主要的桌面应用程序。这些应用程序将产生相当大的网络通讯流量，因此需要更快的网络设备和电缆。

Internet 访问功能和多媒体功能在单位桌面上日益增长的重要性增加了对带宽的需求。一个运行共享应用程序的以太网可能需要传送速度为 100-Mbps 的 5 类 电缆。

对于某个特定的配置应在测试实验室对带宽需求进行评估。例如，如果您的单位计划在数据网络上使用语音和视频，则您的电缆和交换机必须能够满足这些服务的带宽需求。

第三方和内置的 Windows NT 诊断工具能够帮助您确定所需的带宽，如在网络的 WAN 链接上发送压缩的视频信号。然而，在测试实验室中您能够对设备的几种可能配置和操作参数进行测试，来确定其最低的带宽需求。

部署计划会受到要使用的 Windows 2000 功能的配置要求的影响。例如，如果一个分支机构中的 Dfs 卷在速度缓慢的链接上复制到替换 Dfs 卷，您可以决定升级链接以提高带宽或在分支机构中设置替换卷，以减少缓慢链接上的网络通讯。

Windows 2000 的某些功能需要特殊的配置才能实现，如要建立安全 VPN 连接，把 VPN 服务器放置在 WAN 的终端就有帮助。在规划中应考虑配置因素，如怎样集成 VPN 服务器与代理服务器。考虑网络当前的基础结构以及部署 Windows 2000 后希望得到的优势与功能，如使用 VPN 增强 WAN 链接的安全性。有关配置 Windows 2000 安全策略的详细信息，请参见本书中的“ 确定 Windows 2000 网络安全性策略 ”。有关安全的其它信息，请参见本书中的“ 规划分布安全性 ”。

检查网络设备与 Windows 2000 的兼容性。查看网卡、调制解调器和特定类型集线器的硬件兼容列表。例如，Windows 2000 能够将 TCP 校验计算放到支持 Windows 2000 功能的网卡上，改进网络的性能。有关在

HCL 上认可的系统和设备的详细信息，请参见 Web Resources 页的 Microsoft Windows Hardware Compatibility List (HCL) 链接，地址是：
http://windows.microsoft.com/windows2000/reskit/webresources。

Windows 2000 支持异步传输模式 (ATM)，可利用 LAN 仿真 (LANE) 服务提供从传统共享媒体网络迁移到 ATM 的新路径。Windows 2000 也支持 ATM 上的 IP。如果计划使用 Windows 2000 ATM 或正在使用 Windows NT 4.0 ATM，确认 ATM 供应商会提供 Windows 2000 升级驱动程序。确认 ATM 适配器列于 HCL 中。

准备服务器

您可能会在一个混合模式环境中部署 Windows 2000，或最终转移至完全 Windows 2000 网络。您在本书后面部分的“设计 Active Directory 结构”和“确定域迁移策略”中所做的规划，将对与 Active Directory 规划一起实施和升级 IP 寻址规划很有帮助。

您已经标识了基础结构服务器--主域与备份域控制器、DNS、DHCP、WINS 和构成您基础结构的其它服务器。确认硬件已有 Windows 2000 驱动程序。如果所使用的驱动程序或设备不在 HCL 上，应向制造商查询最新的驱动程序，或自己测试它们是否与 Windows 2000 兼容。

旧版本的 Windows NT 和许多第三方 DNS 服务器不能与 DHCP 动态同步，因此不能维护名称和 IP 地址间的不断更新的联系。可以考虑将您的 DNS 服务升级至 Windows 2000–兼容的 DNS。Windows 2000 DNS 可自动更新 DNS 记录字段，因此减少了以前必须进行的人工更新的需要。

准备升级网络时，应根据网络上地理站点的数目和规模以及 WAN 链接的速度和可靠性来考虑您的 DHCP 服务器的存放位置。远程站点间的 DHCP 通信需要增加站点间链接的带宽和可靠性。有关的详细信息，请参见本书中的“确定网络连通性策略”。

如果计划支持使用 NetBIOS 请求来解析 IP 寻址的客户机，您将继续需要 WINS 来解析出计算机名的 IP 地址。通常，MS-DOS®、Windows 3.2*x* 和更低版本、Windows 95、Windows 98、和 Windows NT 系统使用 NetBIOS 来解析 IP 地址。现在您可以开始将 WINS 从您的网络上删除。

Windows 2000 DHCP 通过增强的监视功能、管理单元和多播支持功能来提供多媒体支持。它与 Windows 2000 DNS 动态集成以便支持 Active Directory。旧版本的 DNS 不提供这项支持，如果您计划部署 Active Directory 或想使用网络负载平衡功能来平衡您 DHCP 服务器上的需求，应该考虑将其升级。

安装 Windows 2000 路由和远程访问服务器是实现 LAN-到-LAN 和安全 VPN 链接以及远程访问的必要条件。Windows 2000 集成了路由和远程访问，它支持很多种协议，如：IPX/SPX 和 AppleTalk。

如果在有 UNIX 系统的混合环境中部署 Windows 2000 时，记录当前系统上 BIND 的版本。虽然 Windows 2000 与 BIND 的旧版本完全兼容，但如果使用 BIND 4.9.4 和更高版本可以提供更强的 DNS 功能。

准备域控制器

一些公司计划逐步将 Windows 2000 部署于他们的生产环境中，而另一些公司则准备全面迁移到新系统中。通过将 Windows 2000 安装在单位的部分服务器上，您可以在 Windows 2000 域中维护当前的 Windows NT 4.0 域和信任关系，让您单位有足够时间熟悉 Windows 2000 的操作与概念。有关域迁移的详细信息，请参见本书的“确定域迁移策略”一章。

Windows 2000 可在 Windows NT 4.0 网络中运行。利用 NTLM 协议，Windows NT 4.0 工作站可以向任何一个在 Windows NT 4.0 域中充当域控制器的 Windows 2000 域控制器发送网络身份验证请求。Windows 2000 与 Windows NT 4.0 域之间的信任关系很容易建立，它可支持域间的身份验证。部署 Windows 2000

时，不必将全部 Windows NT 4.0 域同时迁移至 Windows 2000。

将某个域升级至 Windows 2000 时，应首先升级主域控制器。以后您可以根据自己需要把备份域控制器升级至 Windows 2000 域控制器。最后将域添加到 Active Directory 目录树上。您可以从域升级策略中分别升级成员服务器和客户计算机，但如果还没有安装 Windows 2000 域控制器，这些计算机将不能访问 Active Directory 和其它高级功能。

与大部分网络相关的操作过程相同，在升级域控制器时，应准备一个发生故障时使用的恢复所有更改的计划。准备域控制器升级的步骤之一是更新备份域控制器，然后再将其进行隔离，这样它便可以作为一个故障恢复域控制器使用。有关准备故障恢复域控制器的详细信息，请参见本书中的“ 确定域迁移策略 ”。

如果 Windows 2000 域控制器在一个有 Windows NT 备份域控制器的域中运行，该域中的对象（用户、用户组和计算机）总数不应超过 Windows NT 域建议的 40,000。

准备成员服务器

成员服务器是任何一个作为 Windows NT 或 Windows 2000 域成员的服务器，但其角色不是域控制器。成员服务器角色包括：

- 文件、应用程序、打印服务器
- Web、代理和远程访问服务器
- 数据库服务器
- 证书服务器

在成员服务器上安装 Windows 2000 可以增强其角色的功能。

在评估计算机的硬件兼容性时，应记住考虑其升级后要承担的角色。对某特定功能所需的硬件组件要求并没有一个严格的规范。您需要在计算机执行其角色时（最好在测试实验室而不是实际的生产环境中）对其进行测试，看其 CPU 的速度、RAM 和硬盘空间是否满足要求，以及运行其角色的驱动程序、应用程序和协议是否可以达到要求。

有关准备成员服务器的详细信息，请参见本书中的“ 升级和安装成员服务器 ”和“ 服务器自动安装与升级 ”。

准备安全基础结构

Microsoft Windows 2000 的设计既提供高度的数据安全性，同时又便于管理员实施和管理。IPSec、Kerberos 身份验证和公钥等新功能提供了比以前版本的 Windows NT 更高的安全性能。

由于 Windows 2000 可在当前的 Windows NT 域结构中运行，因此很容易将基于 Windows 2000 的服务器加入当前网络安全结构中。然而，在将当前 Windows NT 网络迁移到或升级成 Windows 2000 时，您的安全策略将受到所计划部署的 Windows 2000 的特定安全性能的影响。例如，如果当前网络上使用的是 Microsoft 代理服务器，就需要为 Windows 2000 对其进行升级，并安装适当的客户软件才能使用这项服务。

Windows 2000 提供公钥基础结构 (PKI)，一种使用数字证书、证书颁发机构和证书管理软件的身份验证方法。证书验证可以保护电子邮件客户与 Internet 通讯的安全，它支持智能卡技术，并保证非 Kerberos 客户的通讯（使用 IPSec）安全。有关规划与部署 PKI 的详细信息，请参见本书中的“ 规划公钥基础结构 ”。如何部署 PKI 的细节由所使用的具体证书服务决定--可以使用 Microsoft 证书服务或第三方证书服务。

应定义证书要求、惯例和策略。如果您准备使用第三方 PKI，确认它能与 Windows 2000 兼容。这里，兼容

性意味着能够支持 Windows 2000 中使用根证书层次结构。注意 Windows 2000 PKI 将不会替代当前 Windows 域信任和授权机制，如 Kerberos 协议。Windows 2000 的 PKI 功能被集成到了域控制器和 Kerberos 身份验证服务中。

根据您的优先需要，可以分阶段地实施 PKI 来支持特殊目标，如支持电子邮件或支持当前系统的身份验证。

要分阶段实施 PKI，应该

1. 为域目录林中的每个 Windows 2000 目录树在父域中安装根证书颁发机构。
2. 在每个业务单位域中安装中级证书颁发机构 。
3. 在每个要求安装的站点，在域中为每个用户组安装和配置证书颁发机构与服务。

准备客户

由于 Windows 2000 的设计满足互操作性，运行旧版本 Windows 的客户计算机与混合模式环境中的 Windows 2000 可以互操作。但是，如果将客户计算机升级成 Windows 2000 Professional，可提供增强的客户计算机和用户安全性能、更高的可靠性和更强的功能。

不是所有版本的 Windows 都可以升级到 Windows 2000 Professional。您可以将如下版本的 Windows 和 Windows NT 升级成 Windows 2000 Professional。

Windows 95 所有版本均可进行升级，包括 OSR2.*x*。但如果您的客户从一个服务器上运行 Windows 95，则需要将其直接安装到计算机上或干脆安装 Windows 2000 Professional。

Windows 98 所有版本均可升级。请参见本章后面的“ Windows 2000 Professional 升级的注意事项 ”。

Windows NT 4.0 Workstation 所有版本均可升级。请参见本章后部分的“ Windows 2000 Professional 升级须知 ”。

Windows NT 3.51 工作站 所有版本均可升级。

对客户计算机的一项关键要求是硬件和驱动程序需与 Windows 2000 兼容。

Windows 2000 Professional 升级的注意事项

有些在以前操作系统中工作正常的应用程序与驱动程序在 Windows 2000 Professional 环境中将不能正常运行。以下部分将就升级 Windows NT、Windows 95 和 Windows 98 客户时可能出现的问题展开讨论。

注意 Windows 3.1 或更低版本不能进行升级。

升级 Windows NT 客户

通常 Windows NT 客户考虑如下因素便可以很容易地完成 Windows 2000 Professional 升级：

- 由于 Windows 2000 文件系统模型的更改，依赖于文件系统过滤的任何客户级应用程序将不能正常运行，如防毒或磁盘配额软件。
- 如果客户运行的网络协议在 Windows 2000 操作系统 CD 上的 I386\Winntupg 文件夹中没有升级版本，应考虑是否使用这些协议或寻找 Windows 2000–兼容的新版本。
- 如果您的客户使用第三方电源管理工具，应考虑使用 Windows 2000 高级配置和电源接口 (ACPI)

和高级电源管理 (APM) 来替换。

- 安装 Windows 2000 前删除第三方即插即用驱动程序。

升级 Windows 95 和 Windows 98 客户

Windows 95 和 Windows 98 客户的升级路径一般很简单。但是，在考虑升级这些客户时应注意如下几点：

- 如前所述，依赖于旧文件系统的客户级应用程序将不能正常运行。例如，磁盘压缩、磁盘碎片整理程序将不会工作。防毒应用程序必须与 Windows 2000 相兼容才能正常运行。
- 使用虚拟设备驱动程序 (VxDs) 和 .386 驱动程序的应用程序和工具将不能正常运行。与这些应用程序的制造商联系确定是否有更新驱动程序。
- 许多客户计算机装有第三方设备驱动程序。当安装了这些设备驱动程序时，为了提供其它功能（如配置控制），有时会安装一个控制面板应用程序。请在 Windows 2000 的环境中测试控制面板应用程序并向制造商查询其与 Windows 2000 的兼容性。
- 前面提到的有关网络协议、第三方电源管理工具和第三方即插即用驱动程序应该注意的问题也适用于 Windows 98 和 Windows 95 客户。

准备使用其它系统操作

许多单位使用包含不同操作系统的异机种环境。Windows 2000 Server 为其它操作系统提供了网关服务，许可 Windows 客户获取进入其它操作系统与资源的访问权。例如，通过安装 Gateway Services for NetWare，Windows 客户既可以享受 Windows 2000 网络中的新功能又可以继续浏览 Novell 目录服务 (NDS) 层次结构、使用 Novell 4.*x* 或更新版本的登录脚本和 Novell server 的身份验证功能。

网络基础结构准备任务列表

表 6.1 概括了为 Windows 2000 准备当前网络结构推荐完成的任务。

表 6.1 基础结构准备任务规划列表

任务	章节
创建硬件和软件清单。	硬件和软件清单
确认所有硬件与 HCL 相符且适合部署计划，为每台计算机制定一个明确的硬件升级计划。	硬件和软件清单
记录服务器和客户网络配置。记录基础结构服务器。	网络基础结构
记录网络配置的细节--名称解析服务、IP 寻址、WAN 链接和物理布局。	网络基础结构
创建网络物理和逻辑布局图。	网络基础结构
记录成员服务配置。	文件、打印和 Web 服务器

标识所有关键应用程序并检查其与 Windows 2000 的兼容性。	业务线应用程序
记录域结构和管理模型，包括信任关系、主域控制器和备份域控制器的位置、DNS 的名称空间。	域服务结构
记录网络安全细节。	安全性
稳定网络。	预备步骤
检查网络协议。	预备步骤
准备物理基础结构。	准备物理基础结构
检查网络设备与 Windows 2000 的兼容性。	准备物理基础结构
准备基础结构服务器。	准备基础结构
升级域控制器。	准备域控制器

第 7 章 – 确定网络连通性策略

Microsoft® Windows® 2000 Server 拥有几个新的功能，网络管理员可以使用这些功能来增强他们的新网络或现存网络的基础结构。本章包括关于网络连接问题、地址分配、TCP/IP 和其它一些协议问题的信息。这些信息将帮助用户为自己的单位确定最好的网络连通性策略。

要从本章的阅读中最充分地获益，具备一些关于 Microsoft® Windows NT® 和 Windows NT 网络的知识是有帮助的。用户还需要熟悉基本的或高级的网络概念，如 TCP/IP 寻址、路由协议和远程访问等。

本章内容

网络连通性概述
单位内的外部连通性
Windows 2000 TCP/IP
IP 路由基础结构
Windows 2000 DHCP
Windows 2000 异步传输模式
服务质量
网络策略任务规划列表

本章目标

本章将帮助您撰写下列规划文档：

- 对您的当前网络、协议和路由基础结构的评估
- 网络连通性策略
- 物理网络设计图表
- 网络协议和路由基础结构设计

资源工具包中的相关信息

- 要了解有关 Windows 2000 TCP/IP 的更详细的信息，请参见 *Microsoft® Windows® 2000 Server Resource Kit TCP/IP Core Networking Guide*。
- 要了解有关“ Windows 2000 路由和远程访问 ”的更详细的信息，请参见 *Microsoft*® Windows® 2000 Server Resource Kit Internetworking Guide。
- 要了解关于在 Windows 2000 基础结构中部署安全服务的更详细的信息，请参见本书的“ 确定 Windows 2000 网络安全性策略 ”。

网络连通性概述

在确定如何实施或将用户的网络升级到 Windows 2000 的时候，需要考虑几件事情：如果用户有一个关于当前网络的网络图表，则请参照这份图表来确定在哪里战略地实现 Windows 2000 的新功能。例如：用户需要检查客户、服务器、交换机和路由器来查看当前它们是否在使用如“ 服务质量 (QoS) ”、“ 异步传输模式 (ATM) ”和路由协议等服务。如果有必要的话，还需要检查和修改 TCP/IP 寻址方案，以便利用“ Windows 2000 动态主机配置协议 (DHCP) ”的新选项。

如果您还没有完成上述工作，请首先创建反映您的网络需要的物理和逻辑图表。这是很必要的，因为在采取

任何组网的物理步骤之前，这些图表提供了一份关于基础结构的概述。这使得设计者和管理员可以一起致力于使网络系统和设备到位的工作下面几节将描述用户可在图表中包括的内容。

站点

显示站点在图表中位置的图形描述。它可在用户确定广域和远程连接方法时提供帮助。用户需要依照地理边界、管理边界或上述两者实现站点。

远程连接方法

包括用于把远程站点连接到用户图表中的中央站点的媒体。这包括 T1、E1、帧中继、综合业务数字网 (ISDN) 或普通传统电话业务 (POTS)。用户还可以使用图表来显示用来把站点连接到广域骨干区域的路由器的类型。这些路由器可以是 Windows 2000 路由器或来自不同的第三方供应商的路由器。显示通过直接拨号和虚拟专用网络 (VPN) 技术把远程用户连接到站点的方法。

站点中的内部局域网络连接

创建站点内部网络的图形描述，以便最有效地利用 Windows 2000 的新功能。包括下列信息：

网络媒体：包括用户计划使用的基础结构的类型，如 10 或 100BaseT 连接、ATM 或千兆以太网。如果用户计划使用 ATM，请通过在 ATM 或局域网络仿真 (LANE) 上使用 IP 来确定网络的哪一部分将被直接连接到 ATM 上。

路由和交换基础结构 用户确定将在何处放置路由器和交换机。这对于维护网络带宽和使瓶颈最小化是很重要的。另外，请确保您将使用的路由和交换硬件能够支持如 QoS 等技术。

协议 如果用户计划使用 TCP/IP，请显示站点内每个子网的 IP 寻址方案。如果用户计划使用如 IPX、AppleTalk 或“ NetBIOS 增强型用户接口 (NetBEUI) ”等其它协议，请也将它们显示出来。还需考虑用户可能用来连接用户网络的路由协议，如 OSPF 或 RIP 等。要了解关于 TCP/IP 的更详细的信息，请参见 *Microsoft Windows 2000 Core Networking Guide* 中的 "Windows 2000 TCP/IP"。另请参见 *Microsoft Windows 2000 Server Internetworking Guide* 中的 "Unicast IP Routing"、"IPX Routing" 和 "Services for Macintosh"。

DNS 和 Active Directory 结构 为用户网络设计 DNS 和 Active Directory™ 结构。包括一份逻辑域图表和用户网络图表，用来显示用户的公司中的域和目录林。要了解关于 Active Directory 目录服务的更详细的信息，请参见本书的“ 设计 Active Directory 结构 ”一章。

服务器基础结构 显示 DNS、DHCP 和 WINS 服务器在用户图表中的存放位置。

远程连接方法 显示远程客户和远程网络将如何连接到用户图表中的企业网络。

下面的各节将讨论如何设计一个能够把 Windows 2000 Server 的特性最好地结合到用户的单位中去的网络，并勾勒出了确定网络连通性策略的步骤。

图 7.1 说明了确定用户的网络连通性策略的主要步骤。

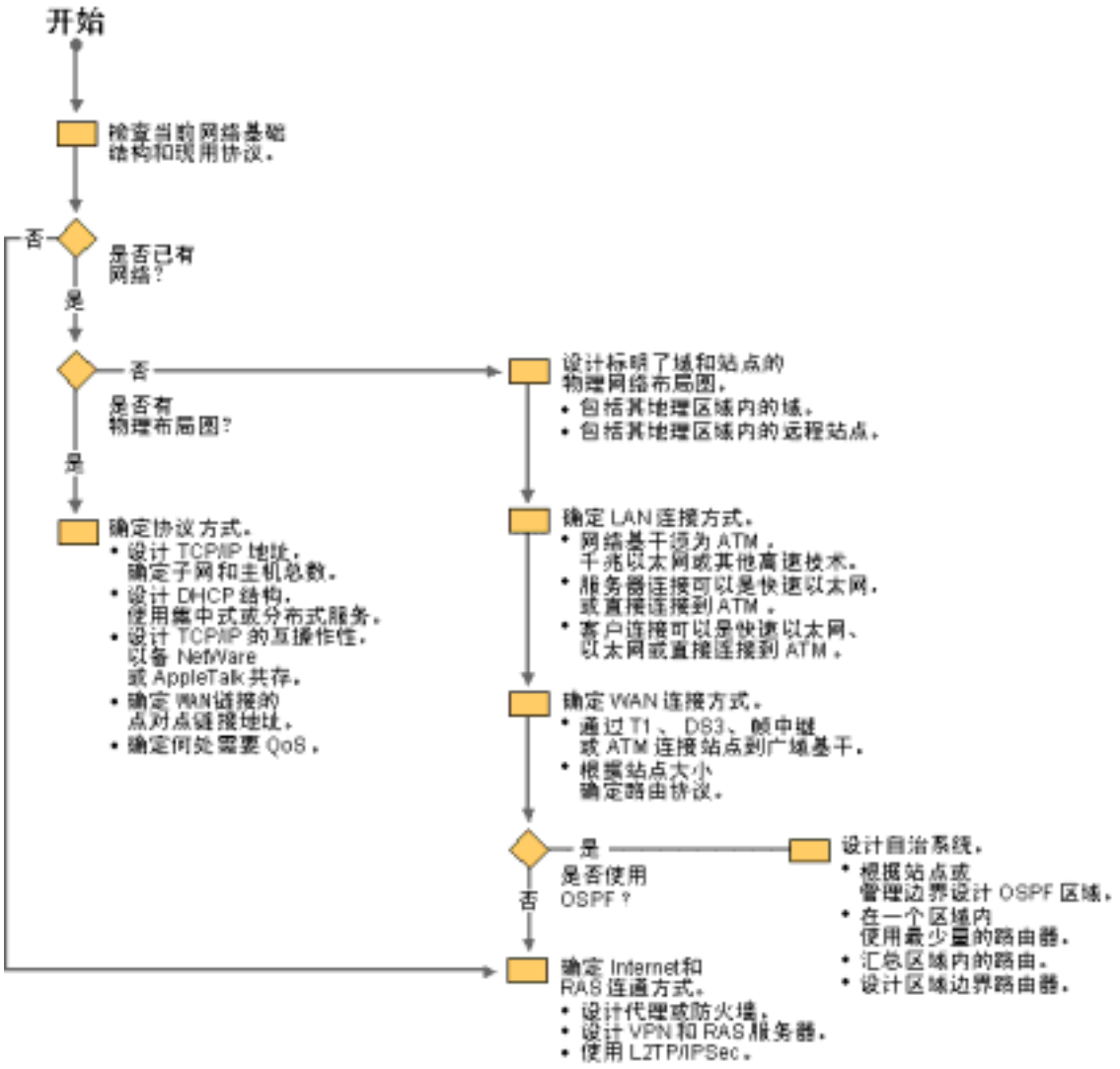


图 7.1 确定网络连通性策略的过程

要为 Windows 2000 设计网络，首先需要设计构成总体基础结构的网络的许多小的部分。下面的各节描述了广域网 (WAN) 的不同方面，以及每个方面的一些步骤和设计注意事项。还包括了企业网络基础结构的外部、广域的方面，如非军事区 (DMZ)、站点实现和远程连接等。还涉及了网络的内部方面，如协议、安全和局域网络 (LAN) 连接方法等。

单位内的外部连接

要让远程用户能够访问中央站点，用户需要部署允许站点到站点的连接和远程客户连接的连接方法。用户单位的中央站点需要拥有一个网络,以便其它站点和远程客户访问中央站点的内部网络结构。下面的各节描述了用户需要在外部连接策略中包括的内容。

设计非军事区

大型企业网络的一个重要部分是 DMZ。本节描述了 DMZ 的用途，本章后面的各节给出了如何使用 DMZ 的范例。

非军事区（DMZ）是一个网络，它允许 Internet 到专用网络的访问,并同时保证该网络的安全。DMZ 使商业机构能够把 Internet 作为节约成本的媒介来使用,同时允许它存在于 Internet 上。DMZ 通过利用 Internet 和 VPN 现有的基础结构来节约金钱，从而节约了租用通信线路的广域连接成本。实质上，DMZ 是一个位于专用网络和 Internet 之间的网络。

DMZ 包含如服务器、路由器和交换机等设备，通过防止内部网络暴露在 Internet 之上来维护安全。DMZ 内的服务器通常包括：代理服务器阵列（网络使用它们来向内部用户提供对 Web 的访问）、外部的“Internet 信息服务（IIS）”（单位可以使用它们来提高单位在 Internet 上的形象），以及所有用来向远程客户提供安全连接的 VPN 服务器。要了解关于 VPN 的更详细的信息，请参见本章后面的“VPN 安全”和 "L2TP over IPSec VPNs" 。

图 7.2 中显示了 DMZ 的一个范例。在 DMZ 边界上的设备是路由器。对于一个大型企业来说，到 Internet 的连接速度最好不低于 DS3 或每秒 45 兆比特(Mbps)。DMZ 中路由器和服务器之间的连接可以是任何高速 LAN，但是如果用户预计会有较大 Internet 流量的话，则使用千兆以太网或 ATM 为宜。

对于小型或中型网络，用户可以在 DMZ 接口上使用“Windows 2000 路由和远程访问”路由器。用户可以在 Internet 接口上启用数据包筛选，以防止不必要的流量并确保安全。

单位的站点连接

很多大型企业都拥有分布在不同的地理位置上的办事处。这些办事处需要一种途径连接到主站点或中央站点，同时保持这种连接。世界各地区使用着不同的广域连接媒体。表 7.1 描述了各种广域技术及其用途。

表 7.1 广域技术

广域技术	定义
T1	以 1.544 Mbps 的速度传输，并由 23 个传输数据的 B 信道和一个用于计时的 D 信道组成。T1 还可以被划分成独立的每秒 64 千字节（Kbps）的片段。
E1	主要在欧洲使用。以 2.048 Mbps 的速度传输。
T3	以 44.736 Mbps 的速度传输 DS3 数据。
帧中继	人们考虑用来代替 X.25 的数据包交换技术。通常以达到 T1 的速度运行。
数字用户线（DSL）	DSL 由一条不对称数字用户线（ADSL）、一条高位速率数字用户线（HDSL）、一条单线路数字用户线（SDSL）和一条极高速数字用户线（VDSL）组成。

站点连接还可以依赖于使用拨号媒体，如“综合业务数字网（ISDN）”或作为低流量链接或后备之用的“模拟电话线路（POTS）”。例如，一个单位可能会有一个通常由一条 T1 分线连接的小站点，但当用户的广域连接出现故障时，用户可以使用后备的 POTS 线路连接。

一个单位内部的多个站点通常通过路由器连接。“Windows 2000 路由和远程访问”提供了路由服务，该路由服务使得单位可以经济地把远程站点连接到中央企业站点上。站点可以使用 VPN 来通过 Internet 连接，从而为用户的单位节约成本。如果用户拥有的站点并不需要在所有时间内都连接到中央站点，则用户就可以实现一个请求拨号型的路由器到路由器的连接，从而节约广域连接成本。

远程客户连接

提高公司工作效率的方法之一，就是使单位用户不论在家还是旅行途中随时都能够访问企业资源。许多企业已经开始采用一种在家工作的策略。该策略节约了雇员上班往返的花销，同时使得企业在雇员增多的情况下，经济有效地管理办公室空间。实现远程客户连接的另一个好处就是，它能够使旅行中的销售和技术人员随时拨入并检索文件和电子邮件。

在上述任一种情况下，不在办公室的用户需要能够连接到他们自己的邮件和文件服务器上，而这些服务器都位于企业网络基础结构中。通过接收远程访问连接并把数据路由到其目的地址，“ Windows 2000 路由远程访问 ”服务能够做到这一点。“ 路由和远程访问 ”服务还能用来接收传入的 VPN 连接，从而提供了一种通过 Internet 的安全的数据传输方式。要了解关于 VPN 的更详细的信息，请参见本章后面的“ VPN 安全 ”和 "L2TP over IPSec VPNs" 。

能访问企业基础结构的远程客户并不仅仅局限于“ Internet 协议 (IP) ”客户。“ Windows 2000 路由和远程访问 ”服务还允许其他客户，如 Macintosh、UNIX 或 NetWare 客户等，通过它的多协议功能来使用远程访问。

Windows 2000 PPTP 中支持的 VPN 协议和“ 第二层隧道协议 (L2TP) ”也支持通过 Internet 的多协议连接。

Windows 2000 TCP/IP

当今，单位中的网络要求一种高性能且具有可扩展性的协议，并高度强调 Internet 互操作性。TCP/IP 协议是一套工业标准协议，是跨越 LAN 和 WAN 的大规模互连网络的基础，并正很快成为企业内部网和 Internet 上的主流协议。

Windows 2000 TCP/IP 是：

- 一种基于工业标准的网络协议。
- 一种可路由的网络协议，支持把基于 Windows 的服务器和客户连接到 LAN 和 WAN。
- 一种可扩展的协议，用来把基于 Windows 的服务器和工作站与异类系统集成在一起。
- 访问全球 Internet 服务的基础。

Microsoft TCP/IP 提供了基本和高级功能，使得运行 Windows 2000 的计算机可以与运行其它操作系统（如 UNIX）的计算机连接并共享信息。

Windows 2000 TCP/IP 套件的新功能

为了保证可靠性和性能，新的 Microsoft TCP/IP 套件具有自我调节功能。下面的四节讨论 TCP/IP 套件的新功能。

自动配置专用 IP 地址

“ 自动专用 IP 地址 (APIPA) ”配置就是在从 169.254.0.1 到 169.254.255.254 的范围内自动地分配一个唯一的地址，当没有 DHCP 服务器时使用子网掩码 255.255.0.0。APIPA 可用在单独的子网中，如 SOHO 网络等（这种网络太小，以致于不适合运行一个独立的 DHCP 服务器）。

例如：如果用户拥有家庭办公室并需要一种方式把 IP 地址分配到内部的 Windows 2000 服务器和客户，这

时只需把系统通过网络媒体连接到一起，然后每台 Windows 2000 计算机就会在 APIPA 地址范围中为自己分配一个地址。

大窗口支持

大接收窗口支持增加了每次连接时可存储在缓冲区中的数据量，从而减少了网络流量并加速了数据传输。

注意 默认时并不启用大窗口支持。窗口默认大小是大约 16 千字节 (KB)，这是 Windows NT 4.0 的窗口大小的两倍。

选择确认

选择确认使得接收者可以通知发送者仅重新传送未收到的数据，而不必重新传送整个数据块。这就使得网络带宽的使用更加有效率。

提高的往返时间估计

TCP 使用往返时间 (RTT) 来估计发送者和接收者之间的往返通信需要的时间量。Windows 2000 TCP 为了设置传输定时器 而对 RTT 作出了更好的估计，从而提高了TCP 的总体性能。TCP 中的这项改进主要在跨越很长距离的 WAN 中有帮助，或在速度过慢的链接中（如卫星通信）有帮助。

Microsoft TCP/IP 规划注意事项

如果用户的网络还没有使用 TCP/IP，那么用户需要为自己的网络开发一个综合的 IP 地址规划。在规划用户 IP 基础结构时，请包括 IP 网络 ID 和子网掩码。请使用下面各节中的信息来创建一个可行的规划。

IP 地址类别

选择将使用的地址类别，这取决于用户的网络是专用的还是连接到 Internet 之上的。网络地址还取决于用户基础结构的大小，而用户基础结构的大小又与使用哪个地址范围直接相关。为用户网络规划 IP 地址时，请注意下列事项：

物理子网和主机清单 计算在当前用户网络中包含的子网和主机的数目，随后通过对用户的 IP 地址建立子网来确定新建网络中所需的子网和主机数。做这项工作时，请预先规划好至少五年的增长，以免地址和子网不会过早用光。如果用户的网络直接连接到 Internet，那么用户将需要一个由用户的“ Internet 服务供应商 ”分配的 IP 地址范围。要了解关于对 IP 地址建立子网的更详细的信息，请参见 *Microsoft Windows 2000 Server Resource Kit TCP/IP Core Networking Guide* 中的 "Internet Protocol Security"。

注意 只让用户网络中的部分 TCP/IP 系统（如 DMZ）和 Internet 相连，这一点是很重要的。从 Internet 上可以访问的系统越少，则用户的网络在面对攻击时就越安全。

带/不带到 Internet 的代理连接的专用网络 对于未连接到 Internet 的专用 TCP/IP 网络或通过代理服务器连接到 Internet 的专用 TCP/IP 网络，用户能够使用 A、B 或 C 地址类型中的任何有效的 IP 地址。但是，为防止在最终连接到 Internet 时还需要对用户的网络重新编号，建议用户使用专用地址。专用 IP 地址空间指由“ Interent 授权号码委员会 (IANA) ”留出的三个 IP 地址集合。保留的 IP 范围是：

- 10.0.0.1/8 到 10.255.255.254/8
- 172.16.0.1/12 到 172.31.255.254/12
- 192.168.0.1/16 到 192.168.255.254/16

注意 要了解关于专用地址的更详细的信息，请参见 RFC 1918。这里显示的专用网络地址范围使用了网络前缀符号，又称作“无类别域间路由（CIDR）”符号，用来定义子网掩码。

子网掩码和自定义子网

在公共 IP 地址短缺的情况下，用户可以使用自定义的子网掩码来实现 IP 子网的建立。自定义子网指子网建立、“无类别域间路由（CIDR）”或变长子网掩码（VLSM）。使用自定义子网，用户能够摆脱默认子网掩码的局限，并可以更有效地使用用户的 IP 地址范围。

通过自定义子网掩码长度，用户可以减少实际主机 ID 使用的位的数目。在某些情况下，用户可以使用标准 A、B 和 C 类网络的默认子网掩码。默认子网掩码是用小数点分割的十进制整数，它能够把网络 ID 同 IP 地址的主机 ID 分隔开来。例如：如果用户拥有一个网段，使用 A 类 IP 地址，范围从 10.0.0.0 开始，那使用的默认子网掩码就是 255.0.0.0。通常，网络接受子网掩码的默认值而不带特殊的要求，这里每个 IP 网段对应一个单独的物理网络。

注意 为防止寻址和路由问题，请确保任何网段上的全部的 TCP/IP 计算机都使用相同的子网掩码。

用户还可以使用网络前缀符号，通过用户的 IP 地址显示子网掩码。这样做可以显示缩短的子网掩码，但它的值仍保持不变。表 7.2 描述了该过程。表 7.2 中有下划线的位组成了网络前缀。

表 7.2 网络前缀长度子网掩码

地址类型	二进制的子网掩码	等价的十进制网络前缀
A 类	11111111 00000000 00000000 00000000	/8 = 255.0.0.0
B 类	11111111 11111111 00000000 00000000	/16 = 255.255.0.0
C 类	11111111 11111111 11111111 00000000	/24 = 255.255.255.0

TCP/IP 和 Windows Internet 命名服务

“Windows Internet 命名服务（WINS）”是一个把网络基本输入/输出系统（NetBIOS）名称映射到 IP 地址的服务。在比 Windows 2000 更早的 Windows 版本中，WINS 用来与 DHCP 一起注册 NetBIOS 名称，并和 WINS 数据库一起注册动态分配的 IP 地址。在这种情况下，一台启用了 DHCP 的主机查询 DHCP 服务器以获得 IP 地址，DHCP 服务器随后把一台 WINS 服务器作为 DHCP 选项分配给 DHCP 客户。在 DCHP 客户租用分配过程结束以后，NetBIOS 名称和与它关联的 IP 地址都由 DHCP 客户在 WINS 数据库中注册了。Windows 2000 提供 DNS 和 WINS 之间的集成。如果某台 Windows 2000 DNS 服务器不能解析一个完全合格的域名（FQDN），则它把这个 FQDN 变换成 NetBIOS 名称并查询一台已经配置好的 WINS 服务器。WINS 服务器返回的 IP 地址被转发给 DNS 客户。

在 Windows 2000 中，如果用户只使用 Windows 2000 服务器和客户的话，则在 TCP/IP 上无须 WINS 和 NetBIOS。如果用户使用如 Windows NT version 3.5*x*、Windows NT 4.0、Windows 95、Windows 98 或 Windows 3.*x* 等系统的话，则仍然需要 WINS，因为这些操作系统使用 NetBIOS 名称解析和 NetBIOS 会话来创建文件和打印共享连接。

WINS 设计注意事项

如果需要 NetBIOS 名称解析，则域中的每个站点都需要拥有至少一个 WINS 服务器。用户可以把这个 WINS 服务器安装在与 DNS 服务器相同的系统上， 或者独立安装。用户还需要在网络中的其他位置安装一个备份 WINS 服务器。用户可以把这个备份 WINS 服务器安装在与 Windows 2000 域控制器相同的系统上，或者独立安装。

路由和远程访问

路由/路由选择，是一个通过使用网络数据包中的地址信息来确定该数据包为到达其目标地址应走的路径的过程。当源主机和目标主机位于不同的逻辑网络中的时候，需要路由选择。在更大的网络基础结构中，也需要路由选择，因为对于整个网络，只使用一个地址集合是不实际的。这是由于随着网络规模的增大，寻址复杂度也会增加。另外，把所有的系统都放在同一个逻辑网络上的一大型网络中，这也是不切实际的。因为这会造成很大的网络流量。

用户可以通过把 IP 地址范围划分成子网来对 TCP/IP 网络进行分段。一旦 IP 地址被分割开，新形成的子网就会通过路由器来把数据从一个子网转发到另一个子网。用户还可以使用路由选择来连接不相似的网络，如以太网、ATM 和令牌环网等。

路由表用来跟踪从一个子网的主机到另一个子网主机的路由。随着网络规模的增大，基础结构内的路由器的数目和路由表的大小也会增加，如果管理员需要跟踪这些路由，他们必须不断地监视网络以发现那些脱机的路由器、或暂时发生故障的链接，随后把这些信息手动输入到路由表中。在网络发生变化时，路由器通过工业标准路由协议来动态地更新路由表。

Windows 2000 Server 向商业提供了 LAN 到 LAN 的路由，并通过集成 Windows 2000 Server 中的“ 路由与远程访问 ”服务为购买专用路由器硬件提供了一个选择方案。通过利用内建的路由协议，该服务支持 TCP/IP 动态路由、网际数据报交换 (IPX) 和 AppleTalk 通信。“ 路由和远程访问 ”服务还可以通过广域连接提供远程办公室连接。

Windows 2000 路由和远程访问服务的新功能

本节讨论“ Windows 2000 路由和远程访问 ”服务的新功能，该服务允许商业及与之相关的远程访问客户通过以 Internet 为数据路径来更安全地发送和接收数据。Windows 2000 网络结构内的客户能够享受从 Internet 获得多播数据的益处。

表 7.3 描述了“ Windows 2000 路由和远程访问 ”的新功能。

表 7.3 “ Windows 2000 路由和远程访问 ”的新功能。

功能	描述
Windows 2000 Active Directory 集成	允许通过使用基于 Active Directory 的工具（如“ 路由和远程访问 ”管理工具）来浏览和管理“ 远程访问 ”服务器。
“ Microsoft 质询握手身份验证协议 (CHAP) ”版本 2	强安全凭据传递和加密密钥生成。该协议专门用来验证使用 PPTP 协议的 VPN 连接。
可扩展的身份验证协议 (EAP)	允许把第三方身份验证方法插入到 Windows 2000 点到点协议 (PPP) 实现中去。内建的 EAP/传输层安全措施 (TLS) 支持智能卡的部署，以实现安全身份验证和强加密密钥生成。

宽带分配协议	通过动态地添加和去除链接以容纳通信流量的变化，从而实现了更有效的多链接 PPP 连接。这一点对于按带宽使用来收费的网络是有用的。对于 ISDN 信道和类似的通信技术来说，也是有用的。
远程访问策略	使管理员能够依照当天的时间、组成员身份、连接类型和其它标准来控制连接。
第二层隧道协议 (L2TP)	提供了客户到网关和网关到网关的 VPN 连接，由“网际协议安全 (IPSec)”提供安全。
IP 多播支持	支持“Internet 组员协议 IGMP 版本 2”，并以多播转发路由器的方式工作，这就允许在连接的客户和 Internet 网络或企业网络之间转发 IP 多播通信。
网络地址转换 (NAT)	向中小型网络提供一个连接到 Internet 的单独的接口，并在公用地址和专用地址之间提供 IP 地址翻译服务。此外，还向内部网络客户提供 IP 地址分配和 DNS 代理名称解析服务。
Internet 连接共享 (ICS)	向小型网络提供一种容易配置但有限的接口，用来把 SOHO 客户连接到 Internet。ICS 提供 DNS 名称解析、自动地址分配，并为 IP 地址分配提供 IP 地址范围。

远程访问策略

在 Windows NT 3.5*x* 和 4.0 版本中，远程访问授权基于“用户管理器”或“远程访问管理”工具中的一个简单的“**赋予用户拨入的权限**”选项。“回拨”选项也在基于每个用户的基础上配置。在 Windows 2000 中，授权是基于用户帐户和远程访问策略的拨号属性来进行的。远程访问策略是一组条件和连接设置的集合，它们使网络管理员在对连接尝试授权时有更大的灵活性。“Windows 2000 路由和远程访问”服务和“Windows 2000 Internet 身份验证服务 (IAS)”都使用远程访问策略来确定是否接受连接尝试。在上述两种情况中，远程访问策略都存储在本地。此时策略在基于每个呼叫的基础上制定。

通过远程访问策略，用户可以依照当天的时间或本周的日期、依照远程访问用户所属的 Windows 2000 组、依照请求的连接（拨号网络或 VPN 连接）类型等等来决定是否授予权限。用户可以配置限制最长会话时间的设置，指定身份验证和加密的强度，设置“带宽分配协议 (BAP)”策略等等。

由于有了远程访问策略，一个连接只有在连接尝试的设置至少与远程访问策略之一匹配时才能得到授权（满足用户帐户拨号属性、以及远程访问策略的配置文件属性）。记住这一点是非常重要的。如果连接尝试的设置不能满足远程访问策略中的至少一条，则不管用户帐户的拨号属性如何，该连接尝试都将被拒绝。

远程访问设计注意事项

下面是一些设计远程访问方案时的注意事项：

- 如果用户已经安装了 DHCP 服务器，那么请配置“路由和远程访问”服务器，以便使用 DHCP 来为远程访问客户获取 IP 地址。
- 如果用户没有安装 DHCP 服务器，请使用静态 IP 地址池来配置“路由和远程访问”服务器，该地址池是一个远程访问服务器附属子网的地址的子集合。

- 如果是在配置 IPX，则请配置远程访问服务器，以自动地把相同的 IPX 网络 ID 分配给所有的远程访问客户。

VPN 安全

许多企业都很关心网络安全，Windows 2000 网络使用两个协议保证 Internet 上的安全通信，即点对点隧道协议 (PPTP) 和用于与网际协议安全 (IPSec) 关联的 L2TP。Microsoft TCP/IP、PPTP 和 L2TP/IPSec 提供最高等级的安全，保护主机与网关之间的路径。

虚拟专用网络的优点

下面的列表包含了使用 VPN 连接而非长途直拨连接的好处。

降低企业一般管理成本 一般管理成本是大企业主要关注的问题之一，而且话费是企业一笔相当大的开销。使用 Internet 作为连接媒体以代替长途电话服务可以降低话费并减少硬件需求。例如，客户只需呼叫本地 ISP，然后，L2TP 和 IPSec 允许用户获得与 Internet 相联的 Windows 2000 VPN 服务器的安全连接，该服务器提供路由和远程访问服务。

减少一般管理费用 因为本地电话公司拥有并管理支持 VPN 连接的电话线，这样就减少了网络管理员的管理工作。

更多的安全 Windows 2000 使用标准的、交互性的身份验证和加密协议，这些协议保证数据在 Internet 上不安全的环境中是隐藏的，而企业用户则可通过 VPN 对这些数据进行访问。而且，如果使用 IPSec 对 VPN 隧道进行加密，Internet 将只能看到外部 IP 地址，而内部地址将得到保护。也就是说，电脑黑客很难破译通过 VPN 隧道发送的数据。

点对点隧道协议 VPN

PPTP 是一种针对客户隧道需求的出色的解决方案。相对于 L2TP/IPSec，它的安装比较简单，而且当它与一个用户名称/强密码方法一起使用时，可以提供很好的安全性。PPTP 是 Windows NT 4.0 最先支持的一个工业标准协议。该协议使用 PPP 的身份验证、压缩和加密。PPTP 在今天的网络上仍得到广泛的使用。因为 L2TP 与 IPSec 能够提供更有力的安全措施，本章将更深入地讨论 L2TP 和 IPSec 加密。

IPSec VPN 上的 L2TP

IPSec VPN 上的 L2TP 使得企业可以通过 Internet 传输数据，同时保持对数据高等级的保护。需要访问企业网络的小规模或远程办事处的客户可以使用这种类型的安全连接。通过使用本地 ISP 并创建进入企业总部的请求拨号型连接，用户还可以将 IPSec VPN 上的 L2TP 用于远端站点的路由器。

当决定在何地和如何设计 IPSec 之上的 L2TP 时，请记住 Internet 访问点或网络的 DMZ 就是 VPN 服务器应存在的地方。VPN 服务器负责加强用户访问决策，该决策可以配置在 Windows 2000域控制器内的用户帐户上、VPN 服务器的远程访问策略和拨号用户配置文件上、或配置在IAS 内。

L2TP 创建必要的 IPSec 安全策略，以保护隧道通信。用户无须在任一计算机上指派或激活自己的 IPSec 策略。如果计算机已经有一个IPSec 策略，L2TP 仅向当前策略增加一个安全规则以保护隧道通信。

L2TP 部署注意事项

为了确保一个 IPSec 上的 L2TP 成功连接，需要在 VPN 客户计算机和 VPN 服务器计算机上安装计算机证书。客户请求 VPN 连接之后，根据用户帐户上的拨号属性和远程访问策略准予 VPN 访问。在 Windows

NT 4.0 中，管理员仅需在“**用户管理器**”或在“**域用户管理器**”中的拨号属性中选择“**准予用户的拨入权限**”，以允许使用远程访问。

在 Windows 2000 中，管理员可以根据 VPN 服务器上和 IAS 内的远程访问策略决定是否允许到企业网络的访问，帮助用户更好地定义安全设置。有了远程访问策略，一个连接被接受的条件是：此连接的设置至少匹配一个远程访问策略。如果不匹配，该连接将被拒绝。

在部署大型的远程访问 VPN 时，可以使用“连接管理器”和“连接管理器管理工具包”，给单位中所有远程访问客户提供一个连接到 VPN 的预配置拨号设置。这样用户单击即可拨号连接到 VPN，使通常情况下的两到三个步骤合并成了一步。

L2TP 示例

以下是几个可以使用 L2TP 的情境。

持续型连接路由器到路由器 VPN 当两个路由器都是通过持续性 WAN 连接，如 T1、T3、帧中继和电缆调制解调器连接到 Internet 时，一个路由器到路由器 VPN 的典型用途是用来连接远端办公室。在这种配置类型中，只需在每一个路由器上配置一个简单的请求拨号接口。一天 24 小时内都可以建立或拆除永久性连接。图 7.2 描绘了一个路由器到路由器 VPN。

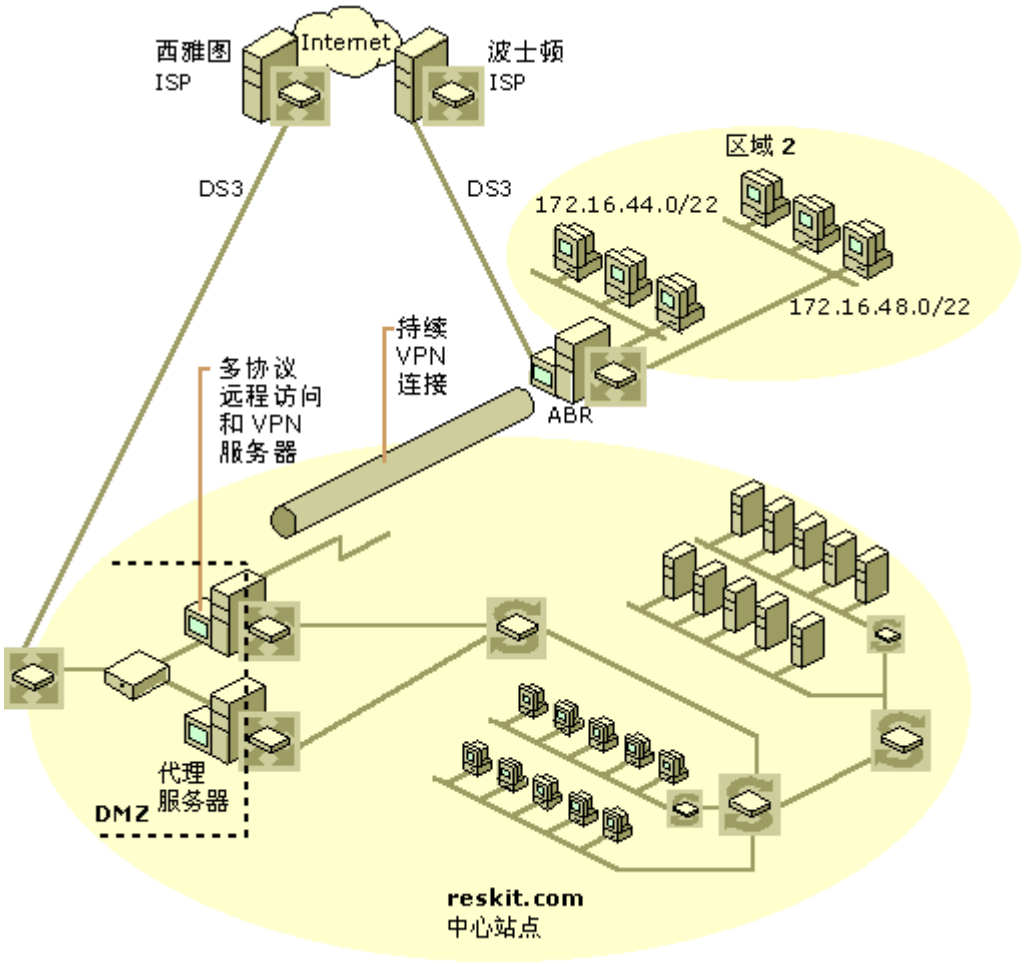


图 7.2 路由器到路由器 VPN

请求路由器到路由器 VPN 当由于位置或费用等原因无法建立一个永久性 WAN 线路时，可以配置一个请求路由器到路由器 VPN 连接。这需要将应答路由器永久性地连接到 Internet。可以通过一个拨号连接（如模拟电话线或 ISDN ）将此应答路由器连接到 Internet。然后，只需在此应答路由器上配置一个简单的请求拨号接口。

具有 IPSec 的 VPN 安全

IPSec 需要部署在位于企业 DMZ 处的 VPN 服务器上。图 7.3 所示的设计表示了一个合并了多协议远程访问服务器的 VPN 服务器。这种合并是一种有效的方式，可以使得各网络远程访问部分集合在一起以实现更方便的管理和安全。而且，当客户使用具有 IPSec 的 VPN 拨入企业网络时，由客户来决定使用何种 IPSec 安全策略类型，以及 IPSec 安装在哪一个远程访问服务器上。然后，它根据客户的定义自动建立隧道。

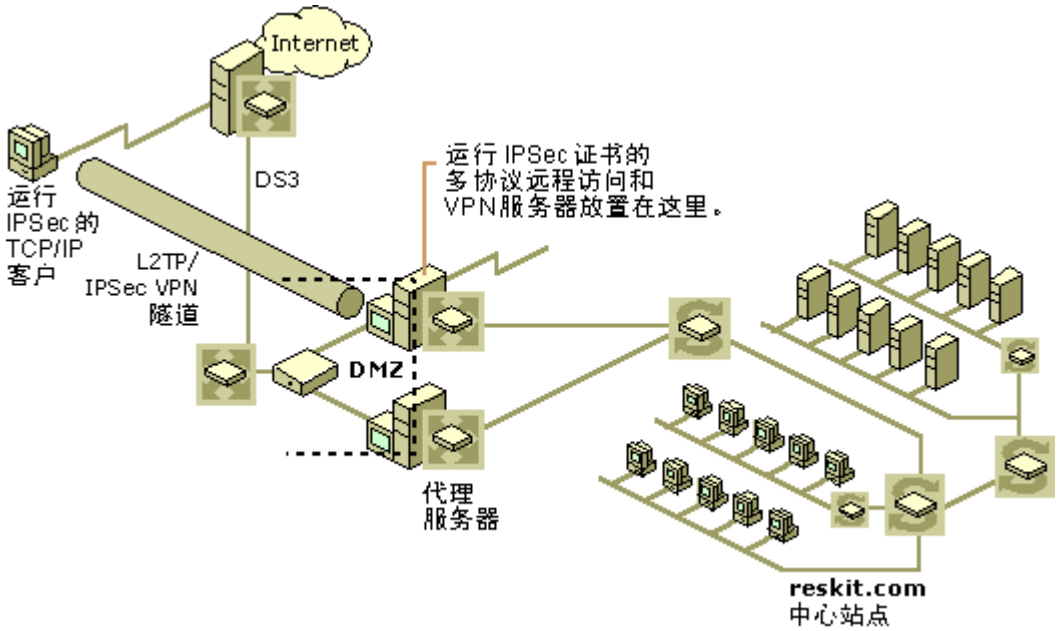


图 7.3 通过 L2TP/IPSec 隧道的路由和远程访问客户连接

在本例中，VPN 服务器有三个接口：一个在 DMZ 内，另一个在与路由器连接的内部网络内，第三个是一个远程访问接口。在 DMZ 内的接口是最不安全的一个接口。如前所述，DMZ 是 Internet 进入内部专用网络的区域，而且应包含所有存在于 Internet 上的服务器。

Windows 2000 执行的 IPSec 基于 Internet 工程部 IPSec 工作组开发的工业标准。

数据加密使企业能够将 Internet 作为一种安全、经济的方式，从远端站点获取信息，或把用户连接到企业基础结构。由于使用的是业已存在的 Internet 媒体，这种策略可以节省费用。安全来自 IPSec。

在 Internet 上，L2TP 将数据放置到一个隧道，IPSec向隧道本身提供安全以保证数据安全，但是应如何处理暴露的接口本身？

可以通过以下方式保护 VPN 服务器上暴露于 Internet 的接口，使之免受电脑黑客的破坏：

- 初始安装 VPN 服务器时，保证 DMZ 内的接口上没有路由协议。相反，接口需要通过一系列综合静态路由指向专用企业网络。
- 在专用网络内的接口上运行路由协议。

- 在 Internet 接口上使用路由和远程访问筛选器（非 IPSec 筛选）为 L2TP 建立输入输出允许筛选器，此筛选器使用用户数据报协议 (UDP) 端口 "Any" 和终点端口 1701。还要为 Internet 密钥交换 （IKE）设置路由和远程访问输入输出允许筛选器，此筛选器使用 (UDP) 端口 "Any" 和终点端口 500，仅允许 IPSec 上的 L2TP 流量。然后，在远程访问策略配制文件中为用户组配置数据包筛选，允许或拒绝某种类型的 IP 通信。为方便用户，在使用路由和远程访问安装程序向导时配置这些筛选器。用户不需做任何配置。

对 IPSec 上的 L2TP 连接，IPSec 安全协商 (IKE) 对计算机本身进行基于证书的身份验证。L2TP 执行用户身份验证的方式可以是通过域\用户名和密码，也可以是通过使用可扩展身份验证协议 (EAP) 的智能卡、证书或令牌卡。关于如何替代这个默认做法以及如何用预共享的密钥进行身份验证，请参见 *Microsoft Windows 2000 Server Internetworking Guide* 中的 "Virtual Private Networking"。

IPSec 要求用户通过使用发给每个计算机的证书来建立信任关系。例如，domain.com 中的一个销售人员与 reskit.com 有常规销售事务。为了加快定购过程，此销售人员每周拨号进入 Reskit 的供应部门下载产品定单表格。

为了保证所有交易免受竞争对手 domain.com 的破坏，此销售人员使用 IPSec VPN 上的 L2TP 通过一个 ISP 拨号进入 reskit.com。远程客户和 VPN 服务器都需要有一个发给他们的证书，而且能够信任他人的证书。为了与 reskit.com VPN 服务器协商信任关系，销售人员的计算机需要安装一个计算机证书。通常情况下，当销售人员的计算机被连接到 domain.com 时，就可以从 Windows 2000 证书服务器上接收到一个证书。该计算机还可接收到一个组策略设置，该设置包含一个名为 “ 证书自动注册策略 ” 的有关到 domain.com 证书服务器上注册的说明。公钥基础结构 (PKI) 证书策略还明确指出：客户可以信任发给 VPN 服务器证书的证书服务器（可能指的是 reskit.com 证书服务器）。 VPN 服务器被配置为信任 domain.com 证书服务器，所以它将接受客户提供的证书。

为 L2TP 完成 IPSec 安全关联后，将检查销售人员的远程访问策略。这是一个允许用户帐户在域内远程访问的属性。如果需要更详细的控制用户访问，可以使用 Internet 验证服务 (IAS) ，这是一个使用 “ 远程访问拨入用户服务 ” (RADIUS) 协议来沟通访问策略的服务器。

用户还可以使用 IPSec 来确保只有具有合法证书和身份的特定计算机才能连接到其他计算机。访问控制列表 (ACLs) 中明确列出的 Windows 2000 用户 ID 和用户组将决定谁能访问特定的共享。

注意 还可以通过企业网络内部使用 IPSec 来加密客户之间的数据和客户到服务器的数据。

关于 IPSec 的详细信息，请参见 *TCP/IP Core Networking Guide* 中的 "Internet Protocol Security"。

Internet 验证服务和集中管理

在大型企业网络中，多个远程访问服务器上的管理策略允许任务频繁。IAS 帮助网络管理员实现在一个中心位置上管理地域分散的远程访问服务器。

IAS 提供：

集中用户身份验证 IAS 支持这样的能力， 即通过认证 Windows NT 4.0 和 Windows 2000 域内的用户，集中管理用户策略。进行用户验证时，IAS 支持多种身份验证协议。包括：

- 密码身份验证协议 (PAP)
- 质询握手身份验证协议 (CHAP)
- Microsoft 质询握手身份验证协议 (MS-CHAP)

- 可扩展的身份验证协议 (EAP)

外包远程访问 使用本地 ISP 网络以允许雇员通过 VPN 隧道连接到企业网络。IAS 允许跟踪连接到 ISP 的费用和用户，这样就可以根据所使用的服务向 ISP 付费。这种方法可以帮助企业节省费用。

远程访问服务器的集中管理 IAS 允许网络管理员仅在一个远程访问服务器上配置远程访问策略，然后，其他远程访问服务器作为 RADIUS 客户从 IAS 服务器上获得策略。

可扩展性 大型企业和 ISP 里的中小型网络可以使用 IAS。

远程监视 通过使用事件监视器或网络监视器，或者通过安装简单网络管理协议，网络管理员可以在网络的任何位置监视 IAS 服务器。

导入/导出 IAS 配置 网络管理员可以使用命令行工具导入或导出 IAS 配置。关于 IAS 的详细信息，请参见 *Microsoft Windows 2000 Server Internetworking Guide* 中的 "Internet Authentication Service"。

多宿主

一个配置了多个 IP 地址的计算机被称为多宿主系统。可以根据需要以几种方式实现一个多宿主系统。用户可把 DHCP 服务器变为多宿主系统，以便向多个子网提供服务。由于 DNS 服务可以在单个接口启动并可绑定到指定的 IP 地址，DNS 也可以受益于多宿主。默认情况下， DNS 绑定到计算机上所有已配置的单个接口。

多宿主的支持有以下几种方式：

- 为每块网卡配置多个 IP 地址
- 多块网卡

IP 路由结构

为了使用户和管理员充分利用 Windows 2000 Server 作为路由器的功能，需要分析网络结构并决定何种路由结构最能满足本企业的需要。表 7.4 描述不同类型的路由配置及其使用。

表 7.4 路由配置

路由配置	描述
静态路由互连网络	使用手动添加路由器到路由网络通信。
针对 IP 互连网络的路由信息协议 (RIP)	使用针对 IP 的 RIP 在路由器之间动态传送路由信息。
开放最短路径优先 (OSPF) 互连网络	使用 OSPF 路由协议在路由器之间动态传送路由信息。

静态路由网络

静态路由 IP 互连网络不使用诸如针对 IP 的 RIP 或 OSPF 等路由协议在路由器之间动态传送路由信息。所有路由信息存储在每一路由器的路由表中。如果决定使用静态路由，应保证每一个路由器在其路由表中存

在合适的路由，以保证 IP 互连网络中任意节点间可以相互通信。

可以使用本章前面所述的网络图表来记录网络结构中的任意静态路由，这是一种理想的方式，可以保证路由的有序化，以作将来参考之用。通过使用路由和远程访问管理控制台，将静态路由输入到 Windows 2000 路由器中的路由表中。关于增加静态路由的详细信息，请参见 *Microsoft Windows 2000 Server Internetworking Guide* 中的 "Unicast IP Routing"。

在使用路由服务前，需要在管理控制台内对其进行配置和启动。关于启动和配置 Windows 2000 路由和远程访问服务的详细信息，请参见 Windows 2000 Server 的联机帮助。有关安装和升级 Windows 2000 成员服务器的详细信息，请参阅本书中的“ 安装与升级成员服务器 ”。

可以在小型网络中实现静态路由，小型网络（如少于 10 个网段的小型企业）几乎不需要管理，而且随时间变化不大。但是，由于它们仍需一定的管理，用户可能认为它们不实用，特别是具有了 Windows 2000 的路由和远程访问服务能力后—该服务可以使用开放式最短路径优先 (OSPF) 或针对 IP 的 RIP 为小型或大型网络动态建立路由信息表）。

针对 IP 的 RIP 网络设计

针对 IP 的 RIP 是一个距离向量路由协议，在相临路由器之间动态传送路由信息，自动根据需要添加和删除路由。RIP 有一个等于 16 的跃点限制。所有跃点等于或大于 16 的目标都被认为是不可到达的。中小型基础结构，如中等大小的企业或办事处，最宜安装 RIP 网络。

其他在网络中使用针对 IP 的 RIP 的忠告包括：

- 针对 IP 的 RIP 使用跃点记数来作为最优路由的指标。比如说，如果一个站点有一条 T1 线路和一条卫星备份线路，而且与这两条线路相关的费用相同，则针对 IP 的 RIP 自由选择任一条线路。为了防止这种问题，可以对慢线路（卫星）配置两倍的费用，这将迫使路由器选择 T1 线路作为主要线路。

- 因为 RIP 路由器每 30 秒发布一次可到达网络的列表，所以还需考虑带宽消耗。根据网络的大小，这些信息发布可能耗尽昂贵的 WAN 带宽。而且，拥塞的可能性也随着网络规模的扩大而增加。可以使用自动静态 RIP 更新来减少路由协议所用带宽。

Windows 2000 路由和远程访问服务支持针对 IP 的 RIP 的版本 1 和版本 2。RIP 版本 1 用于分类环境，不为每个路由发布子网掩码。如果网络中的路由器只支持 RIP 版本 1，而您希望使用无类别域间路由 (CIDR) 或变长子网掩码 (VLSM)，需要升级路由器以支持 RIP 版本 2，或者跳过 RIP 使用 OSPF。

可以使用以下步骤实现针对 IP 的 RIP：

1. 参照网络图表，确定 RIP 路由器将被放置于何处。如果没有当前图表，请考虑在开始前设计一个。考虑将路由器放置于高带宽网络以减少拥塞。 决定准备使用哪一个 IP 地址方案。记下哪些地址用于路由器、哪些地址用于服务器、哪些地址用于客户。例如，如果使用专用地址范围 172.16 0.0/22，可以遵循表 7.5 所示的格式。

表 7.5 IP 地址方案

路由器	地址
172.16.4.0/22 网络上路由器 1 的接口	172.16.4.1
172.160.8.0/22 网络上路由器 2 的接口	172.16.8.1

172.16.4.0/22 网络上的域控制器	172.16.4.10
172.16.8.0/22 网络上的域控制器	172.16.8.10
172.16.4.0/22 网络上的客户	172.16.4.20
172.16.8.0/22 网络上的客户	172.16.8.20

3. 下一步，决定在每一个接口上准备使用 RIP 的哪一个版本。如果正在建立一个新网，请考虑只使用 RIP 版本 2，因为该版本支持 CIDR 和 VLSM。如果有一个使用 RIP 版本 1 的现存网络，请考虑升级到 RIP 版本 2。

OSPF 网络设计

针对 IP 的 RIP 可以方便地将路由协议集成到小型或中型网络环境中。但是，如果您要实现一个大型网络，针对 IP 的 RIP 可能就不够了。Windows 2000 路由和远程访问支持的另一种路由协议叫做开放最短路径优先 (OSPF)。一个 OSPF 网络最适用于一个大于 50 个网络的大型结构。

OSPF 是一个链接状态路由协议，它通过建立一个最短路径树来计算路由表项目。OSPF 比 RIP 更有效，而且没有 16 跃点计数限制问题----此问题导致数据经过第 16 跃点后被丢弃。OSPF 网络可以有一个值为 65,535 的累积路径费用，这个值允许建立非常大的网络（最大生存时间值为 255）并为费用的允许值指派一个大范围。OSPF 还支持点对点专用连接、广播网络（如以太网）、以及非广播网络（如帧中继）。使用 OSPF 的一个缺点是，配置 OSPF 比其他路由协议（如 RIP ）更复杂。

可以分层建立这些网络。下面的部分将更详细的描述 OSPF。

自治系统

一个自治系统是所有共享一个公用管理颁发机构的网络的集合。当设计一个 OSPF AS 时，推荐以下指导方针：

- 将 AS 细分到 OSPF 区域。

  将 AS 分区，这样 OSPF 可以控制通信以最大利用其只通过域内通信的能力，同时保持到 AS 内其他区域的通信为最小。

- 指派基干区域为一个高带宽网络。

  创建一个具有高带宽能力的基干，以保证域内拥塞为最小。

- 保证所有域间通信通过基干。避免创建将新的或正在变化的区域连接到基干的虚拟链接。

图 7.4 描述了一个 AS。

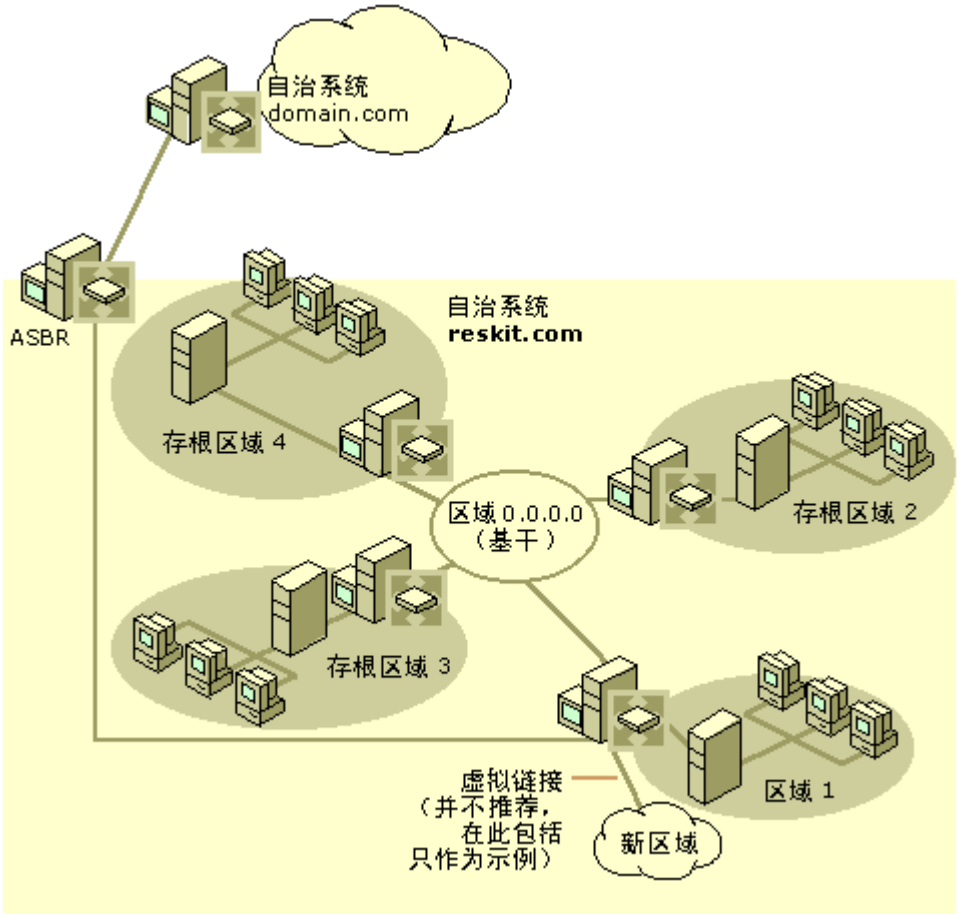


图 7.4 自治系统

OSPF 区域设计

OSPF 区域是 OSPF AS 的一部分，OSPF AS 包含子网的连续集合。区域是那些用来分离站点、域或组的管理边界。这些区域内是网络，当这些网络通过基干连接起来时组成一个 AS。

在内部网中，配置这些区域使得区域间的通信量最小。这包括 DNS 名称解析通信和 Active Directory 复制通信。

通信离开和进入一个 OSPF 区域的一种方式是通过一个叫做地区边界路由器（ABR）的路由器。该路由器连接到被称为 Area 0.0.0.0 的基干，该基干将 OSPF 区域连在一起。 ABR 通常有一个在基干地区网络上的接口。但是，在某些情况下 ABR 无法物理地连接到一个基干网段。在这种情况下，可以通过一个虚拟链接将新的 OSPF 区域连接到基干。虽然这种方法可以达到目的，但由于配置起来较复杂并且容易出错，所以不推荐使用这种方法。图 7.5 显示基干、地区和虚拟链接。

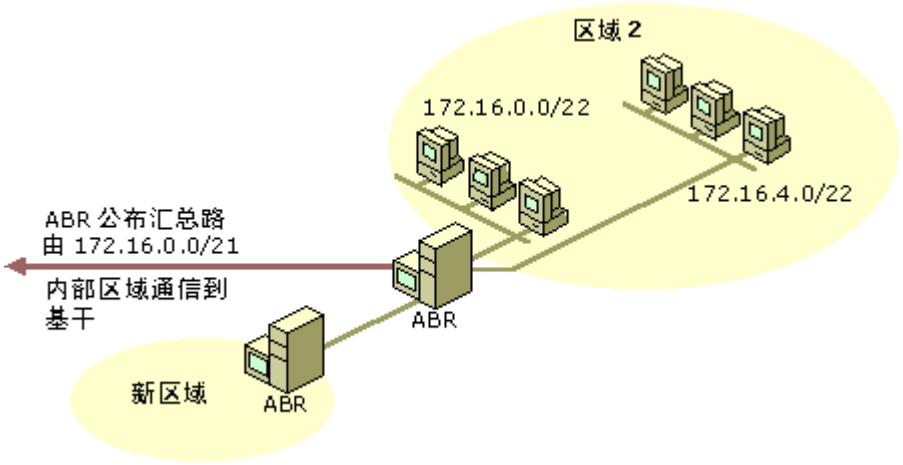


图 7.5 OSPF 区域设计

设计 OSPF 区域时请遵循下列指导方针：

- 以连续方式分配 IP 地址，并允许汇总这些地址。路由汇总是指压缩 IP 地址的范围。理想情况下，一个地区的 ABR 将把它的所有网络 IP 地址汇总为一个。这种方法浓缩了路由信息，减少了 ABR 的工作量和 OSPF 路由表项目的数量。

  只要有可能，请创建存根区域。牢记以下条目：

  - 可以配置存根区域，使得所有外部路由和目的地在 OSPF AS 外部的路由被一个静态默认路由总结。
  - 存根区域不能承载任何 AS 外部的路由（外部路由），包括使用其他路由协议的路由。这意味着存根区域无法使用 AS 边界路由器 (ASBR)。

- 避免创建虚拟链接。虚拟链接被用来把 AS 中的新区域连接到基干。虚拟链接会引起路由和其他问题，且配置起来较困难。通常应努力将 AS 中的新区域直接连接到基干。在实现 AS 前进行预先规划可以保证这一点。

IPX 路由结构

使用 NWLink、NetWare 客户服务和 NetWare 网关服务，可以确保同一网络内 NetWare 服务器和 Windows 2000 系统的互操作性。Windows 2000 Server 提供的服务可以使 Novell NetWare 网络与服务器共存和相互操作。Windows 2000 包括 NWLink IPX/SPX/NetBIOS 兼容传输协议 (NWLink)。该协议提供 Windows 2000 和 Novell NetWare 系统之间的连接。在混合环境中使用 IPX/SPX 和启动 IPX 路由的理由是：

- 可能需要 Windows 2000 路由器提供 NetWare 客户和服务器之间通信的路由选择。
- Windows 2000 客户可能需要获得 NetWare 服务器的服务。

Windows 2000 路由支持针对 IPX 的 RIP，该功能非常类似于针对 IP 的 RIP 和针对 IPX 的服务广告协议 (SAP)，它们给予节点（诸如文件服务器和打印服务器）通告服务名称和 IPX 地址的能力。作为服务主机的服务器周期性的发出 SAP 广播，IPX 路由器和 SAP 服务器接收此广播并通过每 60 秒发布一次的 SAP 公告传播服务信息。

IPX 网络设计

IPX 网络 ID 是一个 4 字节的标识符，表示为一个 8 位十六进制数。该网络 ID 必须是唯一的，不然 NetWare 客户会发生网络连接问题。4 字节的 IPX 网络 ID 是一个地址空间，可以用它来把多个 IPX 网络组成一组：

内部和外部网络 内部网络是虚拟网络，存在于 Novell NetWare 服务器、Windows 2000 服务器和其他作为服务主机的 IPX 路由器内。内部网络的指派确保获取这些服务的正确的路由选择。

不同以太网帧类型网络 对于需要支持多种以太网帧类型的 IPX 环境，需要用其各自的 IPX 网络 ID 配置每一种以太网帧类型。

远程访问网络 当使用一个运行 Windows 2000 的计算机作为远程访问服务器时，远程访问客户被指派一个 IPX 网络 ID。默认情况下，远程访问服务器选择一个唯一的 IPX 网络 ID。可以指定一个 IPX 网络 ID 或一个 IPX 网络 ID 范围，这样远程访问 IPX 通信就可以通过其源 IPX 网络地址确定。

部门或地理位置 可以根据地理（如建筑物或站点）或部门（如销售或开发）分配部分 IPX 地址空间。比如说，在某大型校园环境内， 5 号楼内的所有 IPX 网络可以使用 5 作为它们地址的第一位。

最大直径 针对 IPX 的 RIP 和 SAP 的最大直径是 16 跃点，对于针对 IP 的 RIP 也是如此。直径是一个互连网络大小的度量标准，按照一个数据包到达其终点必须通过的路由器数量加以衡量。超过 16 跃点的网络和服务被认为是不可到达的。

限制和指引 NetBIOS-over-IPX 通信 可以通过在特定接口禁用 NetBIOS-over-IPX 广播传输和配置静态的 NetBIOS 名称来控制 NetBIOS-over-IPX 通信。比如说，如果一个特定 IPX 网络内不含有任何使用 IPX 上的 NetBIOS 的节点，则可以在所有连接到此网络的路由器上禁用 NetBIOS-over-IPX 的广播传输。

防止 SAP 广播传输 在 IPX 网络上使用服务广告协议 (SAP) ，以告知网络客户可用的网络资源和服务。如果 SAP 广播不需在整个互连网络内传输，可以使用 SAP 筛选来防止 IPX 服务发向 IPX 网络组外的广告。比如说，如果需要隐藏人力资源部的文件服务器，可以配置连接到该部门的路由器，从而过滤掉有关该部门文件服务器的文件和打印共享服务。另外一个理由是，这样做可以减少发到不需 SAP 服务的子网上的通信。

AppleTalk 路由结构

Macintosh 操作平台上的网络依赖于 AppleTalk 协议组。这些协议包括内置式路由能力，利用此能力可以在 AppleTalk 互连网络内建立路由器。

多播支持

媒体服务在 Internet 和专用网络上正变得越来越普遍。Windows 2000 TCP/IP 支持多播通信的转发，Windows 2000 路由和远程访问服务作为路由器支持 Internet 组管理协议 (IGMP)。主机使用 IGMP 加入一个多播组。路由和远程访问 IGMP 启动接口可以用下列两种方式之一进行操作：

- IGMP 代理模式接口转发从其他运行在 IGMP 路由器模式下的接口产生的 IGMP 报告和多播通信。
- IGMP 路由器模式接口接听来自主机的 IGMP 通信，并在适当情况下更新 TCP/IP 多播转发表，同时发出 IGMP 询问。

Windows 2000 Server 提供的 IGMP 代理是被用来从单个网络 intranet 向 Internet 多播允许部分传送 IGMP 成员身份报告数据包。

可以在企业结构的 DMZ 内安置 IGMP 代理路由器，从而向内部网络主机提供来自 Internet 的视频和音频通信。确保 IGMP 路由器是在一个具有快速切换的高带宽网络上，以尽量减少拥塞。DMZ 内的 VPN 服务器也可以用做 IGMP 路由器，但只能用在小型网络结构中，这时服务器不会因为远程访问和多播通信而导致过载。

当配置 IGMP 接口时，代理模式下的接口面对启用多播的 Internet ，而路由器模式下的接口面对内部网络。图 7.6 显示了一个例子。

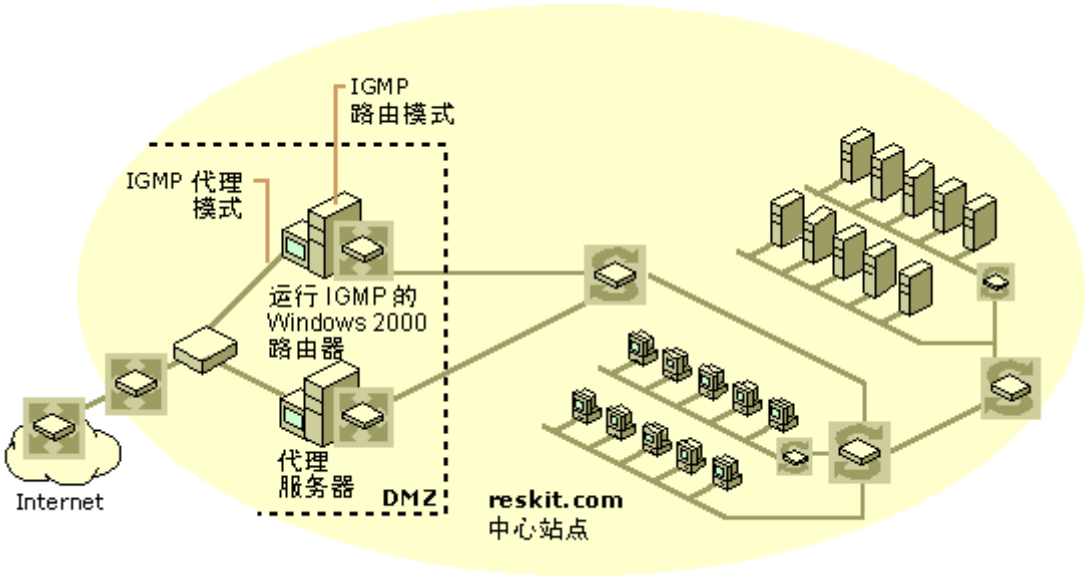


图 7.6 代理模式下的 IGMP 接口

注**意** 图 7.6中的例子只有当符合下列条件时才可行，即：把 Windows 2000 IGMP 路由器连到 Internet 上的硬件路由器是多播允许的，而且 ISP 位于多播基干上。

网络地址转换

Windows 2000 网络地址转换 (NAT) 允许小型网络[如一个小型办公室/家庭办公室 (SOHO)]上的计算机共享一个 Internet 连接。已安装 NAT 的计算机可以用作网络地址转换器、简化的 DHCP 服务器、DNS 代理和 WINS 代理。NAT 允许主机计算机共享一个或多个公共注册 IP 地址，这将有助于保存公用地址空间。

有两种连接到 Internet 的类型：路由和转换。当规划路由连接时，需要从您的 ISP 那里获取一个用于网络内部的 IP 地址范围以及需要使用的 DNS 服务器的 IP 地址。既可以静态配置每个 SOHO 计算机的 IP 地址，也可以使用 DHCP 服务器。

Windows 2000 路由器需要与内部网络(比如说,10 或 100BaseT 以太网)的网卡共同配置。还需要同 Internet 连接一起配置，如模拟的或 ISDN 调制解调器、*x*DSL调制解调器、电缆调制解调器或部分 T1 线路。

转换方式(或称 NAT)提供了一个更加安全的网络,因为专用网络的地址对 Internet 是完全隐藏的。使用 NAT 的共享连接的计算机负责 Internet 地址与专用网络间的双向转换。但应当认识到的是， NAT 计算机没有转换所有负载的能力。这是由于，某些应用程序在除了标准 TCP/IP 标题域外的其他域内也使用 IP 地址。

- 以下协议无法与 NAT 协同工作：
- Kerberos

- IPSec

NAT 中的 DHCP 分配器功能允许所有 SOHO 网络内的 DHCP 客户从 NAT 计算机自动获得一个 IP 地址、子网掩码、默认网关和 DNS 服务器地址。 如果网络上有非 DHCP 计算机，就需要静态配置它们的 IP 地址。

为了尽量降低 SOHO 网络的费用，只需要一个 Windows 2000 服务器。根据您是否运行转换或路由连接，该服务器可以满足 NAT、APIPA、路由和远程访问或 DHCP。

关于 NAT 及其配置的详细信息，请参见 Windows 2000 Server 联机帮助。

Windows 2000 DHCP

TCP/IP 网络上的每一计算机都需要唯一的名称和 IP 地址。Windows 2000 动态主机控制协议 (DHCP) 提供一个简化和自动完成此过程的方式，向网络上的客户提供 IP 地址的动态分配，无论其处于何地或者移动了多远。这样可以减少管理的工作量。

使用 DHCP 的好处

DHCP 通过减少向每一主机手动分配地址的需要，从而实现网络内 IP 地址的可靠分配。这样可以防止 IP 冲突，而 IP 冲突会造成网络的禁用。

移动用户从 DHCP 获益良多，因为 DHCP 允许移动用户移动到网络内部的任何位置，而且当其重新连接到网络时能自动获得 IP 地址。

与 DNS 服务器的互操作性给网络资源提供了名称解析，允许 DHCP 服务器和 DHCP 客户向 DNS 注册。

Windows 2000 DHCP 的新功能

Windows 2000 DHCP 的新功能允许一种更加灵活和可扩展的方式来向主机分配 IP 地址。以下部分将描述这些新功能。

增强的服务器报表

通过使用显示在 DHCP 管理器中的图标，能够以图示的方式跟踪 DHCP 服务器、作用域和客户的一般状态（亦被称为 "member items" ）。关于该主题的详细信息，请参见 DHCP 管理器联机帮助。

附加作用域支持

Windows 2000 DHCP 协议标准还包括支持 IP 多播地址的分配，多播地址分布的方式与单路地址相同。在多播 DHCP 中，多播作用域的配置方式与标准 DHCP 作用域的配置方式一样，但是 D 类作用域使用从 224.0.0.0 到 239.255.255.255 的范围，而不使用 A、B 或 C 类地址。

多播通常用于视频和音频会议，在这种情况下通常需要用户特别配置多播地址。与要求网络上所有计算机都可到达的 IP 广播不同，多播地址是一组计算机，它们使用组成员身份来确定谁应接收信息。

多播地址分配功能有两部分：服务器端分发多播地址；客户端的应用程序编程接口 (API) 请求、更新和发布多播地址。为了使用该功能，需要首先在服务器上通过 DHCP 管理单元配置多播作用域和相应多播 IP 范围。然后象管理一般 IP 地址那样管理多播地址，这样客户就可以调用 API 来从一个作用域请求多播地址。

DHCP 和 DNS 集成

域名服务器为网络资源提供名称解析并与 DHCP 服务紧密相连。在 Windows 2000 中，DHCP 服务器和客户可以向 Windows 2000 DNS 动态更新协议注册。DHCP 和 DNS 的集成启动 A 类型（名称到地址）和指针 (PTR) 、或地址到名称记录的注册。这将允许 DHCP 服务器作为一个代理，代表 Windows 95 和 Windows NT 4.0 Workstation 客户在 Active Directory 内动态更新注册。

DHCP 和 DNS 集成设计注意事项

在网络上共同使用 DHCP 和 DNS 时，考虑您是否正在使用老式的、静态 DNS 服务器。静态 DNS 服务器无法与 DHCP 动态交互，当 DHCP 客户配置发生变化时也无法保持名称——地址映射信息的同步，在企业内部互连网络中经常从一个子网移动到另一子网的移动用户就是一个例子。在这种环境中最好将所有静态 DNS 服务器升级到 Windows 2000 DNS。

未经授权的 DHCP 服务器检测

Windows 2000 的 DHCP 服务是用来避免未经授权的 DHCP 服务器发生地址分配冲突。不然就会发生下列问题：用户创建的未经授权的 DHCP 服务器向网络上的其他客户分配非法 IP 地址。比如说，用户可以利用非唯一地址创建原想用于本地的 DHCP 服务器，而当网络上的其他客户请求地址时，这个服务器会向非计划中的客户租出地址。

Windows 2000 的 DHCP 服务器的管理功能能够预防未经授权的分配和检测现存未经授权的 DHCP 服务器。过去任何人都可以在网络上创建 DHCP 服务器，而现在则需要一个授权的步骤。经过授权的人员通常是 Windows 2000 Server 操作平台所属域的管理员或者是那些被委派管理 DHCP 服务器任务的人员。

引导协议客户动态支持

DHCP 服务器响应引导协议 (BOOTP) 请求和 DHCP 请求。BOOTP 是一个已建立的 TCP/IP 标准 [RFC 951]，用于 DHCP 之前的主机配置。设计 BOOTP 的最初目的是用来为无盘工作站启用启动配置。这些工作站具备有限的存储和本地检索 IP 地址的能力，以及加入基于 TCP/IP 网络的启动过程所需的其他配置信息。

有了对动态 BOOTP 的支持，就可以为 BOOTP 客户指派一个地址池，其指派方式与作用域用于 DHCP 客户 的方式相同。这将允许动态管理分配给 BOOTP 客户的 IP 地址。还允许 DHCP 服务收回用于动态 BOOTP 地址池中的 IP 地址，但首先应核实特定的租期已到期，且 BOOTP 客户仍在使用每一个地址。

只读控制台访问 DHCP 管理器

当安装 DHCP 服务时，该功能提供添加一个特殊目的本地用户组和 DHCP 用户组。通过使用 DHCP 管理器控制台向该组添加成员，可在服务器计算机上向非管理员提供有关 DHCP 服务的信息的只读访问。允许具有成员资格的用户在本地组内查看（但无法修改）特定 DHCP 服务器存储的信息和属性。当帮助中心“拉”DHCP 状态报告时，该功能很有用。只允许对 DHCP 系统管理员组中的成员赋以读/写访问权。

将 DHCP 设计到网络中

当设计和升级网络时，可以通过使用集中或分布式的方法实现 DHCP。（见图 7.7 和 7.8）。在集中式环境中，IP 地址被集中分配到 DHCP 服务器，一个 DHCP 服务器负责分配相关子网或站点内的地址。在分布式环境中，一个 DHCP 服务器可以负责所在站点或其他本地或远程的任何包括在给定的企业结构中的站点。

为有效规划采取何种地址分配方案，请考虑下面讨论的问题。

网络基础结构的大小

在您的域结构中有多少站点？如果仅有一个中心站点和两个远程站点，最好执行分布式的 DHCP。有三个或更多站点的域结构需要集中式的 DHCP 结构，DHCP 服务器向给定站点分配 IP 地址。

图 7.7 和 7.8 是分布式和集中式 DHCP 环境的例子。分布式环境是用来向远程站点分配 IP 地址。集中式环境是用来在站点内分配 IP 地址。因为 Windows 群集与所有启用群集的 Windows 服务一起工作，其他启用群集的服务可以在已经运行了启用群集的 DHCP 服务的服务器上运行。

在图 7.7 中有两个站点，一个是主/中心站点，另一个是远程站点。两个站点都有一个 DHCP 群集在各自站点分发 IP 地址，没有通过广域链接的 DHCP 通信。

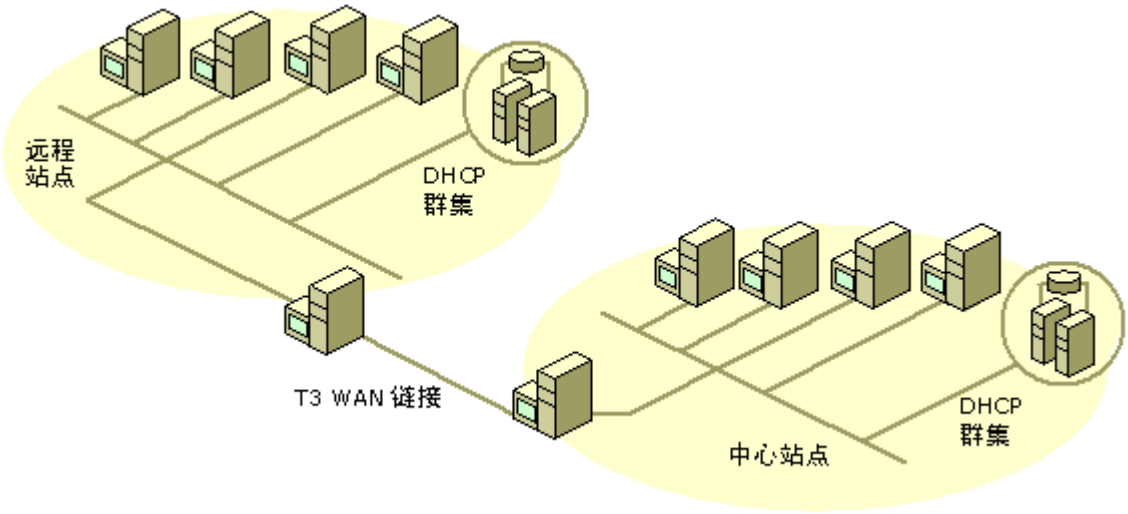


图 7.7 集中式 DHCP

图 7.8 中也有两个站点，中心站点和远程站点，但这次中心站点负责向本身及远程站点分配 IP 地址。注意远程站点有一个备份的 DHCP 群集服务器，它在广域链接失败或出现其他问题时处理 DHCP 通信。

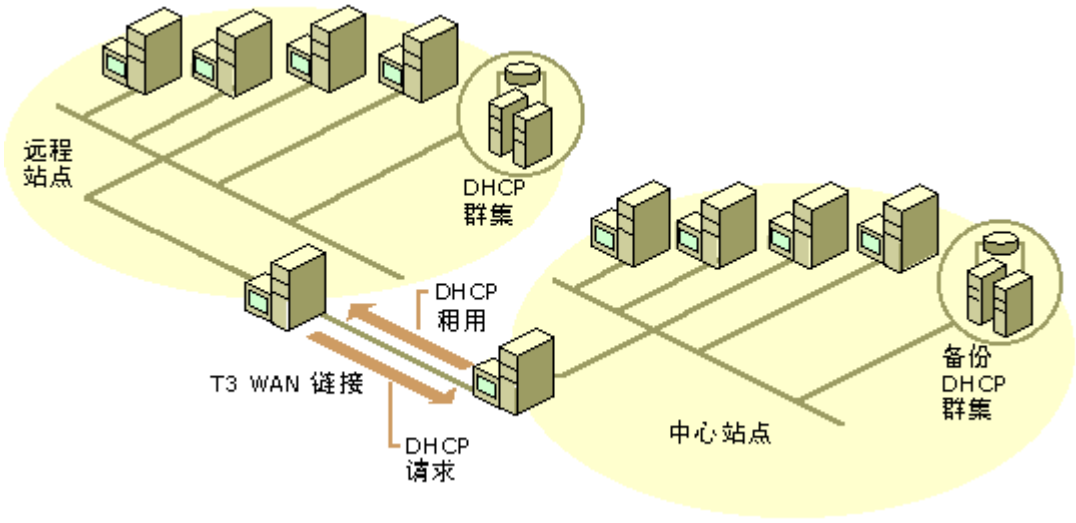


图 7.8 分布式 DHCP

关于 DHCP 的详细信息，请参见 Windows 2000“帮助”和 *Windows® 2000 Resource Kit TCP/IP core Networking*

Guide。

Windows 2000 异步传输模式

在网络支持多种信息类型（如数据、语音和实时视频和音频）的情况下，Windows 2000 ATM 提供一个灵活的、高速的、可扩展的解决方案，以满足网络内服务质量日益增加的需求。有了 ATM，每一信息类型都可以通过单个网络连接。Windows 2000 ATM 服务允许现存网络基干无缝地移植到 ATM，并允许使用 Windows 2000 局域网仿真 (LANE) 服务与传统 LAN 互连。关于 LANE 的详细信息，请参见本章后面的“ Windows 2000 ATM 的功能 ”。

使用 Windows 2000 ATM 的优点

Windows 2000 ATM 有以下优点：

- 高速通信。
- 面向连接的服务，与传统电话相似。
- 快速的基于硬件的交换。
- 单一、通用、可互操作的网络传输。
- 一个网络连接能够可靠地混合语音、视频和数据。
- 灵活有效地分配网络带宽。
- 服务质量 (QoS) 的支持 ，这将使得管理员能够根据几个参数即可分配网络带宽，参数包括（但不限于）以下方面：请求发起人、发送数据的类型（如数据流视频）或目的地。关于 QoS 的详细信息，请参见 *Windows® 2000 Resource Kit TCP/IP core Networking Guide*。

Windows 2000 ATM 的功能

Windows 2000 的新功能允许扩展性更高的框架结构以构建多样的网络结构（如 ATM）。以下部分描述 Windows 2000 ATM 所包括的新功能。

ATM 用户网络界面调用管理器

Windows 2000 现在包括调用管理器，该管理器支持和管理 ATM 网络上的调用。它符合 ATM 论坛 UNI 3.1 版本的信号传输规则，并支持创建交换虚电路 (SVC) 和永久性虚电路 (PVC)。

更新的 NDIS 和 ATM 硬件支持

NDIS 版本 5 现在直接支持 ATM 网卡。这样就允许 ATM 网卡供应商通过编写与 Windows 2000 接口的小型端口设备驱动程序，更加有效的使用其硬件。Windows 2000 中包含了供绝大多数 ATM 网卡供应商使用的驱动程序。

ATM LAN 仿真

ATM LAN 仿真 (LANE) 服务用来提供 ATM 和传统 LAN 环境的互操作。LANE 使得移植和集成传统网络 LAN 技术（如在 ATM 网络上仿真以太网 LAN 和令牌环 LAN）变得更容易。Windows 2000 包括对

ATM LAN 仿真的支持，并可以作为一个 LAN 仿真客户 (LEC) 加入一个仿真 LAN (ELAN)。

Windows 2000 LAN 仿真客户可以通过其 ATM 供应商网络交换机的支持，使用 LAN 仿真服务。默认情况下， Windows 2000 如果检测到已经安装了 ATM 网卡，将安装LAN 仿真客户。默认情况下，LEC 还将试图加入一个默认的未指定的 ELAN。必须为这个默认 ELAN 配置 LAN 仿真服务。

图 7.9 举例说明一个 LANE 网络。

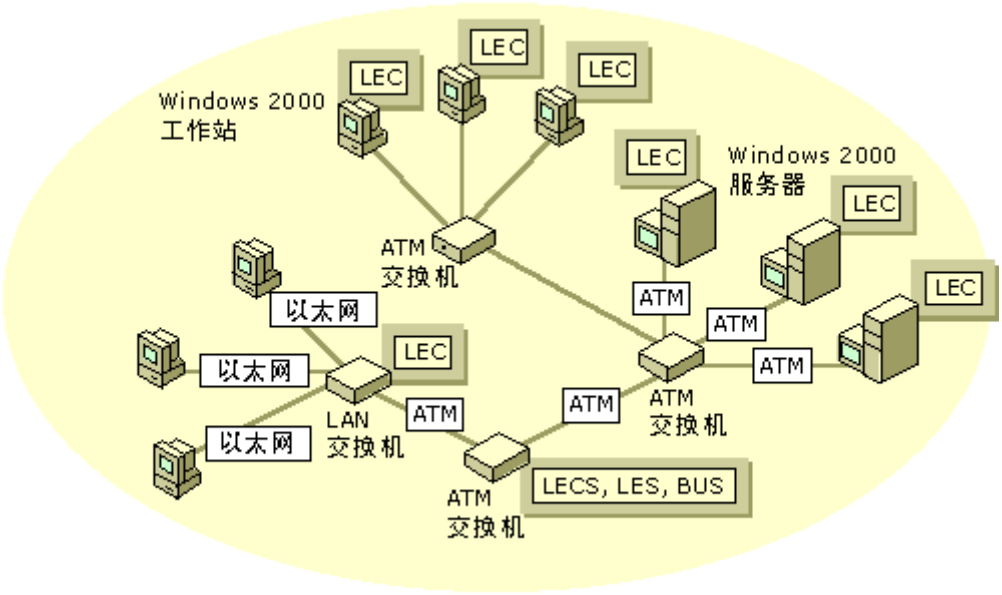


图 7.9 LANE 网络

IP/ATM

IP/ATM 使得 TCP/IP 能够直接使用 ATM 网络的功能。Windows 2000 现在包括 IP/ATM 支持。有了这个支持，为使用 TCP/IP 而编写的应用程序将直接使用 ATM 网络。而且，使用 Windows Socket 下的一般服务质量 (QoS) 的应用程序将直接受益于 ATM 网络本身就能提供的 QoS 能力。

IP/ATM 是一组 ATM 网络上的通信服务，可以用来替代 ATM LAN 仿真。由两个主要组件处理 IP/ATM：IP/ATM 客户和 IP/ATM 服务器。IP/ATM 服务器包括一个 ATM ARP 服务器和一个多播地址解析服务器 (MARS)。IP/ATM 服务器组件可以放置在 Windows 2000 服务器上或 ATM 交换机上。

使用 IP/ATM 的主要优点是它比 LANE 更快，这是由于 IP/ATM 不需在数据包通过协议栈时向数据包添加其他信头信息。一旦一个 IP/ATM 客户已经建立起连接，就可以不加修改地传输数据。

有了 IP/ATM，您既可以使用静态 IP 地址，也可以配置 TCP/IP 文件从而使用 DHCP 服务器。图 7.10 描述一个 IP-over-ATM 网络。

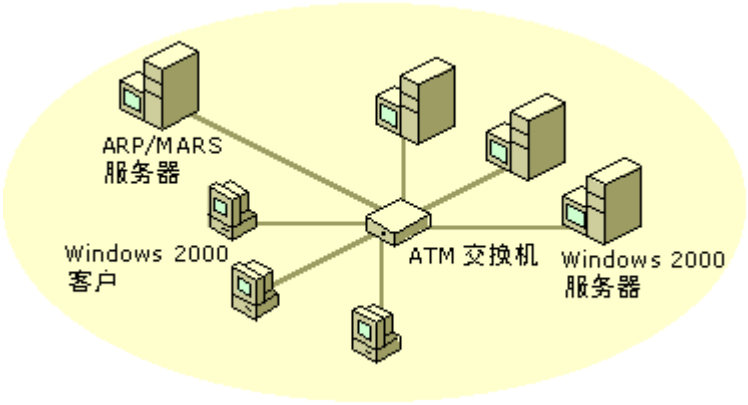


图 7.10 IP/ATM

多播和地址解析服务

Windows 2000 包括多播和地址解析服务以支持使用 IP/ATM。该服务支持 IP/ATM 地址解析协议，并使得 ATM 网络有效地使用多播。

PPP/ATM

随着数字用户线 (*x*DSL) 技术的发展，来自家庭和小型办公室的高速网络访问正在变的越来越普通。在该领域存在几个标准，包括异步 DSL (ADSL) 和通用 ADSL (UADSL 或 DSL Lite)。这些技术在本地环路上运行（电话网络与家庭间的最后一段铜线）。在美国的绝大多数地区，本地环路连接到一个 ATM 核心网络。

*x*DSL 上的 ATM 服务保持高速特性；QoS 在不改变协议的情况下，在核心网络层保证可用性。这就创造了一个潜能，即：使端到端的 ATM 网络延伸到家庭或小型办公室。这种网络模式提供了几个优点，包括：

- 协议透明性
- 有保证的多类 QoS 支持
- 带宽可扩展性
- 通往更新 DSL 技术的演变路径

在这个端到端结构上增加点到点协议 (PPP) 可以增强功能和有用性。PPP 提供以下其他好处：

- 用户级的连接身份验证
- 第三层地址分配
- 到不同目的地的多个并发会话
- 第三层协议透明性
- 加密和压缩

如果每个虚电路（VC）只承载一个点到点协议（PPP）会话，每一个终点将有其自己的已验证的 PPP 会话，它为每一个 VC 提供身份验证。这样就提供了额外的安全措施，如果您有一条专用线路还可以保证带宽。使用 AAL5 上的 Null 封装，将进一步减少信头（因为 PPP 提供协议复用）。

ATM 设计的注意事项

ATM 网络由三个截然不同的组件组成：终端元素（用户）、ATM 交换机和接口。当设计 ATM 网络时请考虑以下部分所讨论的指导方针。

使用默认的ELAN

Windows 2000 ATM 初始配置为一个默认的未指定 ELAN 名称。如果计划实现一个小型的 LAN 仿真，推荐的做法是使用未指定 ELAN 的预配置默认。 如果需要实现一个大型的 ATM 网络，多个 ELAN 将更容易管理且更安全。

当购买 ATM 交换机时，推荐的做法是查阅产品说明书，以保证其使用默认未指定 ELAN 的名称来预配置 ELAN。预配置为默认 ELAN 的交换机可在小型 ATM 环境中减少设置差错。

使用受支持的 ATM 适配器

在购买用于 Windows 2000 的 ATM 适配器之前，应保证它出现在 Windows 2000 硬件兼容列表中。有关详细信息，请参见 Web Resources 页上的 Hardware Compatibility List 链接，其地址是 http://windows.microsoft.com/windows2000/reskit/webresources 。

注意升级前的配置

从 Windows NT 4.0 升级到 Windows 2000 之前，对于每一个计划升级的 LAN 仿真客户来说，应注意以下配置信息：

- ELAN 名称
- LAN 上所仿真的媒体类型
- 与 ELAN 有关的 LAN 仿真服务器 (LES) 以及广播和未知服务器 (BUS) 的 ATM 地址。

配置 ELAN

对这些配置参数进行记录之后，使用 ATM 交换机上的配置接口来配置 LAN 仿真配置服务 (LECS)、LAN 仿真服务 (LES) 以及广播和未知服务 (BUS) ，以支持 ELAN 和相应参数。然后，安装 Windows 2000 并为每一个 LEC 配置 ELAN 名称。

对每一个逻辑 IP 子网只使用一个 ATM ARP/MARS

如果您的网络使用 IP/ATM，推荐的做法是为网络上的每一个逻辑 IP 子网只配置一个 ATM ARP/MARS。如果在同一个网段有多个 ARP 服务器，并且使用这些服务器的地址配置 ARP 客户，则 ARP 缓存将丧失同步。这将导致部分网络无法到达。

服务质量

Windows 2000 服务质量 (QoS) 是一系列组件和技术，网络管理员使用这些组件和技术分配和管理端到端的网络资源。QoS 为下列网络通信保证固定带宽：视频和音频应用程序和 ERP 应用程序，这些应用程序通常使用大量的网络带宽。QoS 是一种允许网络有效控制其通信，并尽可能减少在新硬件资源上所花费用的方法。许可控制服务将使得管理更加方便——许可控制服务是一个 QoS 的管理接口，它允许集中管理 QoS 策略。这些策略决定如何预留和分配优先级带宽，您可以配置这些策略以满足用户、程序和物理位置的要求。过去，QoS 已被集成到路由器和交换机硬件中。现在， QoS 成为 Windows 2000 的一部分，在桌面上就可以实现

对整个企业更新层次的控制。

Windows 2000 QoS 提供以下优点：

- 通过 QoS 许可控制服务管理器的集中式策略和子网配置。
- 使用企业、子网和用户身份作为预留网络资源和设置优先级的标准。
- 保证对用户是透明的优先级带宽，且无须用户培训。
- 保证网络管理员能为优先级通信分配网络资源。
- 提供保证低延迟端到端发送服务的安全措施。
- 与LAN、WAN、ATM、以太网和令牌环配置的互操作性。
- 对带宽保留消息的多播传输的支持。
- Windows 2000 QoS 许可控制简化您对优先级带宽的管理，同时保持低水平的拥有开销。在该实例中，低水平的拥有开销等指的是不需更换网络媒体以获得带宽。

关于 DHCP 的详细信息，请参见 Windows 2000 “帮助” 和 *Windows® 2000 Resource Kit TCP/IP core Networking Guide*。

网络策略规划任务列表

表 7.6 列出了决定网络连接策略时所需完成的任务。

表 7.6 网络策略规划任务列表

任务	章节
检查现存关于连接结构的网络图表。如果该网络图表不存在，请设计一个。	网络连接概述
检查 TCP/IP 结构。	Windows 2000 TCP/IP
决定 Internet、路由以及远程访问的连接方法。	路由和远程访问
决定 WINS 需求。	TCP/IP 和 Windows Internet 命名服务
检查路由以及远程访问的注意事项。	路由和远程访问
检查数据安全的注意事项。	VPN 安全和 L2TP-over- IPSec VPN
检查 IP 路由结构。	IP 路由基础结构
确定多播需求。	多播支持

确定 DHCP 要求。	Windows 2000 DHCP
检查任何服务质量问题。	服务质量

第 8 章 – 使用 Systems Management Server 分析网络基础结构

网络管理员可以使用 Microsoft® Systems Management Server (SMS) 来执行多种 Microsoft® Windows® 2000 部署任务，包括收集规划详细信息、准备计算机、部署 Windows 2000 、监视部署过程。本章重点介绍可用以分析网络基础结构的 SMS 功能。分析结果将有助于确定因准备部署 Windows 2000 而需对网络基础结构所作的更改。使用 SMS，用户可以节省实施企业级部署的成本。

您无需任何使用 SMS 的经验就能理解本章出现的概念和程序。当然，本章不包含部署和使用 SMS 的步骤。有关详细资料，请查阅 SMS 文档。您需要接受过 SMS 培训的人员以周密计划过的方式来正确地部署和使用它。请参阅本章后面的“其它资源”来更好地掌握 SMS。

本章内容

分析网络基础结构
收集清单
使用清单准备网络基础结构
监视网络
确保应用程序兼容性
网络分析规划任务列表

本章目标

本章将帮助您撰写下列规划文档：

- 结合了 SMS 的网络基础结构分析过程
- 包括硬件和软件的现有网络基础结构的详细报告

资源工具包中的相关信息

- 有关使用 SMS 部署 Windows 2000 的详细信息，请参阅本书的“使用 Systems Management Server 部署 Windows 2000”。
- 有关测试应用程序与 Windows 2000 兼容性的详细信息，请参阅本书的“测试应用程序与 Windows 2000 的兼容性”。

分析网络基础结构

部署 Windows 2000 的关键一步是准备网络基础结构。为了使网络做好部署的准备，您需要完成一系列任务，首先是分析网络基础结构的现有状况。

为部署 Windows 2000 而对您的网络进行分析和准备时，需要执行的主要任务包括：

- 标识出那些没有足够的或不兼容硬件的计算机。
- 升级硬件。
- 标识出那些软件与 Windows 2000 不兼容或在 Windows 2000 环境下不能正常运行的计算机。
- 标识出最常使用的应用程序，以便对所有最重要的应用程序进行兼容性测试。

- 分析网络使用情况来确定网络容量可用性、使用的协议和哪些计算机被用作服务器。
- 升级不兼容程序。
- 确保不使用不兼容的应用程序。

Systems Management Server (SMS) 提供您在企业环境下最有效率地执行这些任务所需要的工具。

使用 Systems Management Server

SMS 是一个能用来执行多种计算机管理任务的极具扩展性的系统。部署 Windows 2000 时，SMS 可以加快许多重复任务的执行。图 8.1 显示了用以网络分析和准备的部署规划任务。

备注：在本章中，网络基础结构定义为包括您网络中所有与 SMS 兼容的计算机。其中包括运行 Windows 2000、Windows NT Server、Windows NT Workstation、Windows 95、Windows 98、Windows 3.1 和 Windows for Workgroups 的计算机。

图 8.1：使用 SMS 分析网络基础结构的流程

使用 SMS 来规划和部署 Windows 2000 的过程需要附加资料。当然，自动执行 Windows 2000 部署任务将很容易抵消规划和使用 SMS 的成本。

您可以使用 SMS 立即为最终用户自动执行 Windows 2000 部署任务。即使是首先把计算机加入 SMS 的任务，都不需要技术人员亲临现场。自动执行任务具有如下好处：

- 极大地减少了手工劳动和站点访问。
- 分布地域广阔。
- 出错时容易恢复。
- 日程安排灵活。
- 每天（或更频繁）更新状态。

备注 SMS 依赖于运行在客户机和（至少偶尔）通过网络连接到 SMS 基础结构的软件组件。因此，不能在还不具备操作系统和网络客户的新计算机上用 SMS 安装 Windows 2000。本书中的“客户自动安装与升级”一章提供了在新的计算机上安装 Windows 2000 的方法。

Systems Management Server 如何加快部署 Windows 2000

SMS 通过解答一系列重要问题来帮助您规划部署 Windows 2000。它通过如下方式部署 Windows 2000：

- 准备计算机。
- 分配 Windows 2000 的资源文件给用户计算机。
- 以受控的、安全的方式开始 Windows 2000 的升级。
- 报告部署状态。

SMS 还能帮助您解决有关部署的问题，并且在完成部署后提供一个适当的 Windows 2000基础结构的管理结构。

本章重点介绍如何使用 SMS 来收集用于部署 Windows 2000 所需的有关网络基础结构的详细信息。您可以使用多种报表工具把易于使用的报表中的数据进行格式编排。为做进一步分析，可以把信息提取到其它程序中，如 Microsoft® Excel。而且还可以用收集到的信息自动执行部署任务。收集到的信息有助于解答各种重要的部署规划问题，如：

- 您有多少台计算机？它们的位置如何？它们的硬件是否足以用来支持 Windows 2000？哪些计算机包含与 Windows 2000 不兼容的硬件？
- 您用户的计算机安装了哪些软件？正在使用的是哪些软件？哪些计算机包含与 Windows 2000 不兼容的软件？
- 网络连接的容量有多大？网络使用了哪些协议？

您也会了解 SMS 如何帮助解决应用程序的兼容性问题。

备注 部署 Windows 2000 时使用 SMS 的另一好处是能够把 Windows 2000 发布到要迁移的计算机上，然后开始升级并报告其状态。本书中的“使用 Systems Management Server 部署 Windows 2000”对这些内容进行了详尽的论述。

与 Systems Management Server 1.2 的不同之处

SMS 2.0 与它的前一版本 SMS 1.2 明显不同。两个版本的总体功能近似，但实现各自功能所用的技术大不相同。如果计划用 SMS 1.2 进行网络分析和 Windows 2000 部署，您需要注意它和 SMS 2.0 有以下不同之处：

- 软件清单以预定义的应用程序定义为基础。因此，必须调查您的组织会用到哪些应用程序，然后确认这些应用程序是为 SMS 定义的。虽然 SMS 包含了许多预定义的应用程序，大多数组织仍需要为 SMS 1.2 的软件清单集合定义更多的应用程序，以满足他们的需求。这些定义也可从专家顾问、Internet 以及独立软件开发商那里得到。
- 硬件清单并不全面，因此很难收集到您需要的全部硬件信息。一级计算机制造商具有桌面管理接口（DMI）计算机管理代理，它们提供了广泛的硬件清单信息，可供 SMS 1.2 收集。但每个制造商有不同的解决方案，所以在混合环境里进行部署将非常困难。独立软件开发商提供了解决方案，可在这方面改进硬件

清单。

- 不论从寻找目标还是从执行的角度看，软件分发都不够灵活。
- 所有客户都需要硬件清单。没有和 SMS 2.0 客户发现程序相同的程序。所以，如果客户未通过硬件清单报告，SMS 1.2 就无法同它们一同工作。
- 因为不具备软件测试功能。所以 SMS 1.2 无法阻止用户运行不兼容的应用程序。然而，可以使用第三方软件测试应用程序，而且许多应用程序通过不同的方式与 SMS 1.2 集成。没有提供产品适应性数据库。然而，可以通过定义一个可比较的数据库表来建立一个等价系统。
- 没有 Network Monitor Control Tool （网络监视器控制工具）和 Network Monitor Experts （网络监视器专家），它们是对 Network Monitor（网络监视器）的增强工具。（将本章后面讨论）。
- 如果使用 SMS 1.2，那么要传播 SMS 登录脚本和它们的组件的话，SMS 1.2 将依赖域控制器之间的 Windows NT 复制。

收集清单

分析网络基础结构是从收集硬件和软件的清单开始的。这些数据是部署 Windows 2000 的关键。

评估硬件当前状态

Windows 2000 是为各种各样的计算机设计的。然而，因为这些年来生产了大量不同型号的计算机和组件，因此认为并非所有计算机都能运行 Windows 2000 也是自然的。SMS 可以帮助辨识这些计算机。

硬件容量

最近购买的计算机可能有足够容量来运行 Windows 2000，但老机型可能缺少必要的资源。计算机内存不够、磁盘空间不够、处理器速度过慢、没有 CD-ROM 驱动器、或者处理器太老，都被认为是典型的资源不足。

必须找出资源不够的计算机以便进行升级或更新换代。而且，如果您能预先规划好计算机的分布并能确切知道哪些计算机需要升级，那么将极大提高计算机升级效率。然后，当您到达某个站点时，您会备有正确的组件并直接去到需要处理的计算机。

硬件兼容性

各种各样的硬件细节对于升级规划相当重要。除了通常的磁盘空间、计算机内存和处理器速度问题外，您还需要考虑如下问题：

- BIOS
- 视频卡
- 网卡
- 磁盘控制器
- 电源管理
- 其它硬件如 CPU 芯片集

通常这些组件应该和 Windows 2000 兼容，但不兼容也是可能的。如果供应商能够确认您所购买的计算机和 Windows 2000 兼容，或者在 Windows 2000 Hardware Compatibility List（Windows 2000 硬件兼容性列表）中包含它们，那就不会有问题。在 http://www.microsoft.com 键入关键字“ HCL ”可以查到“ Windows 2000 硬件兼容性列表 ”。否则，您要做先导测试来发现这些问题。先导测试涉及每种型号中适当数量的计算机，在升级依赖于这些计算机的用户之前，您的公司使用的正是这些计算机。

当确定不兼容的型号或组件后，您可以用 SMS 清单功能来找出您公司里其它有同样问题的计算机。通过检查与 Windows 2000 不兼容组件的 SMS 硬件清单详细信息，您可以选择特别标识那些组件的特征，进而选择包含这些组件并可能发生问题的计算机。然后调整硬件报告来查找其它有同样问题的计算机。建议做进一步的测试，来验证所有通过此方法识别的计算机确实有问题且所有问题都已解决。随着您在测试中和对测试结果的信心的增加，您会对基于这些报告的升级的成功更具信心。

使用 Systems Management Server 硬件清单

当您在单位部署 SMS 后，启用 SMS Hardware Inventory 就相当简单。收集硬件清单详细信息的 SMS 客户软件和 Windows 管理规范 (WMI) 组件一起工作，以检查计算机硬件详细信息。WMI 是 SMS 的一部分，而且也有其它来源。客户机自动向 SMS 服务器报告硬件清单详细信息，而且数据向上层传送。这样您便可以从中心位置访问数据。在默认情况下数据每周更新一次，但您可以更改频率。

备注：SMS 是通过叫做“ 发现方法 ”（discovery methods）的过程来查找计算机的。发现程序确能提供一些有关计算机的基本信息，包括它们存在的事实、它们的名称、它们的网络地址和位置。这对于某些硬件清单类型的查询和报告来说可能足够了。和硬件清单相比，发现程序具有所需资源少的优势。当然，资源的差别通常并不重要。

SMS 收集了一套详尽的硬件清单详细信息，其中包括您所需的绝大多数信息。如果需要其它详细信息，SMS 硬件清单很容易扩充。典型的扩充是，询问用户在哪一层，哪一间办公室等等。另一典型的扩充是收集可能包含于 BIOS 里的供应商特有信息，如序号或型号。这些数据通常很难以电子方式收集，无法用标准化的技术获得，或者是依赖于主观偏好；因此需要用户特定扩充。然而，这些扩充如 SMS 文档描述的那样易于实现，。

表 8.1 提供了运行 Windows 2000 可能会有容量或兼容性问题的硬件组件的假想示例。其中包括用于检查这些组件的 SMS 类和属性。下一节讨论如何使用类和值来报告、分析和使用已收集的数据。

表 8.1：Windows 2000 硬件需求示例

资源	Professional	Server	SMS 类	SMS 属性
内存	90 M	128 M	SMS_G_System_X86_PC_MEMORY	TotalPhysicalMemory
磁盘空间	1 G	1 G	SMS_G_System_Logical_Disk	FreeSpace
处理器	Pentium	Pentium II	SMS_G_System_PROCESSOR	Name
视频卡	未标识	未标识	MS_G_System_VIDEO	AdapterChipType

表中的硬件需求值只是假想值，可能适用于一些公司。需求根据用户的不同类型和不同升级路径而不同，而且类似的计算机配置执行起来也不一样。因此，由您自己来判断 Windows 2000 所需的最小需求是很重要的。另外，视频卡通常没有与 Windows 2000 兼容性的问题。以视频卡是否已被 SMS 标识来选择系统升级只是硬件兼容性判断标准的一个例子 — 您会发现因为某个特别的视频卡芯片，或因为 SMS 提供数据的任意数

量的其它硬件详细信息而必须去掉某些计算机。

评估软件当前状态

Windows 2000 包含和以前版本 Windows 相同的编程接口和功能；但是改进的功能并非总是以同样方式运行。兼容性问题通常可以通过不同的编程标准来最小化，但并不是所有应用程序都是严格按照这些标准来开发的。由于这些相似原因，为各种版本 Windows 设计的某些软件可能与 Windows 2000 不兼容。“ 测试应用程序与 Windows 2000 的兼容性 ” 一章对软件兼容性问题进行了深入的论述，对如何确定您的计算机应用程序是否与 Windows 2000 的兼容提供了详细信息。然而，您仍需面对两大问题：“ 您的计算机使用哪种软件应用程序？ ” 和 “ 这些应用程序安装到了哪些计算机上或由哪些计算机使用？ ” SMS 为这些问题提供了答案。

您可以象启动和使用 SMS 硬件清单一样启动和使用 SMS 软件清单。SMS 收集信息的方法是非常不同的，因为它要扫描每个客户计算机的硬盘来查找带 .exe 扩展名的文件。如果它们存在，将再检查这些文件以获得更多详细信息，然后此信息被报告至 SMS 站点服务器。您可以通过配置 SMS 查找扩展名除 .exe 之外（如 .dll 或 .com）的文件，来扩展 SMS 软件清单。

由于 SMS 软件清单收集了有关每台计算机上所有可执行程序的详细信息，您可以相信您能标识安装在您单位的计算机上的所有软件。SMS 软件清单也试图从每个程序提取头文件数据。头文件数据是有关软件的信息，它包含于可执行文件里。近来开发的程序都有头文件数据，但所有计算机都包含一些旧程序。抽取的程序头文件信息提供描述性名称，而不是通常的加密程序文件名。

表 8.1 列出了需要与 SMS 软件清单中的数据一起处理的一些属性。

有头文件数据的软件属性归 SMS_G_System_SoftwareProduct 类。表 8.2：软件数据

数据	有头文件数据的软件	无头文件数据的软件
文件名	FileName	FileName
文件大小	FileSize	FileSize
产品名称	ProductName	N/A
产品版本	ProductVersion	N/A
产品语言	ProductLanguage	N/A

SMS 软件清单能标识安装在计算机上的所有软件，但不能告诉您哪种软件投入使用。当软件不再使用时，也就不再发生升级那些应用程序的成本。SMS 软件清单能从客户机收集文件。如果您有许多装有大文件的客户机，这将加重您网络的负载和占用站点服务器很大的磁盘空间。但是，如果节俭使用，软件清单将是一个强大的工具。比如，您可以在 Windows 95 或 Windows 98 的计算机上运行 Windows 2000 的升级，而只产生一个升级报告（Windows 目录中的 Upgrade.txt）。

为建立一个升级报告，您要用到 **Winnt32 /checkupgradeonly** 命令或一个适当的应答文件，以及本书 “ 使用 Systems Management Server 部署 Windows 2000 ” 所描述的步骤。然后 SMS 软件清单可以为每台计算机收集该文件并将其存储于中央位置，以您方便时查阅。升级报告可能提供有关在升级计算机之前需要解决的硬件或软件问题的建议。

SMS 具有报告实际软件使用的功能，叫做软件测试。软件测试报告每个程序的调用，然后将该数据记录在 SMS 站点数据库中。操作系统附带的程序，如 Notepad 的数据通常不被收集。

Microsoft® Systems Management Server Administrator's Guide 中的 “Metering Software”一章描述了如何使用 SMS 软件测试，包括如何建立基于数据的报告。请特别考虑使用脱机模式，这种模式下收集的信息相同，但报告不够频繁。这将大大降低网络、客户机、服务器的负载。

使用清单准备网络基础结构

当收集完所有数据，您就可以用它们来解决因规划 Windows 2000 部署而产生的问题。也可以用这些数据加速部署进程。

报告收集的数据

使用 SMS 清单数据的主要方法是建立回答具体问题的报告。有关建立 SMS 报告的更多信息，参见 Web 资源页的 Microsoft Systems Management Server Technical Details 链接，地址是：
http://windows.microsoft.com/windows2000/reskit/webresources。

部署 Windows 2000 需要建立如下报告：

- 具有运行 Windows 2000 所需容量的计算机
- 与 Windows 2000 兼容的计算机

  执行 Windows 2000 升级的技术人员可以用这两个报告来标识哪些计算机可能需要硬件升级。

  当两个问题都有的话，可以结合使用这两个报告。
- 需要硬件升级的计算机

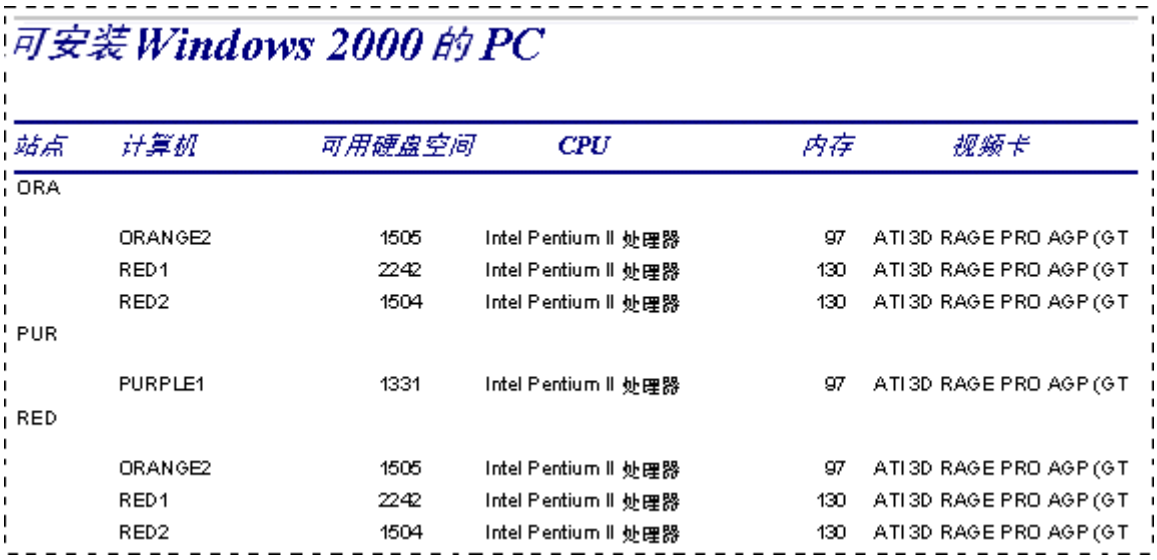
  这可供正在执行硬件升级的技术人员来订购合适的硬件并标识需要升级的计算机。
- 需要软件升级的计算机

  这供正在执行软件升级的技术人员来订购合适的软件并标识需要升级的计算机。

每个报告可按站点分列数据，或尽可能地细化，这取决于你单位如何充分使用这些信息。

Windows 2000 就绪的 Systems Management Server 报告示例

下面的查询要用表 8.1 所列的 SMS 类来查找已经作好 Windows 2000 升级准备的计算机。这种情况下使用的标准是 C：驱动器有 1G 的可用空间，计算机内存至少 90M 且用Pentium 处理器，视频卡不是未标识的（即不等于空字符串）。这些标准假定 C：驱动器是用户的系统分区。这个示例查询产生的报告在图 8.2 中显示。



可安装 Windows 2000 的 PC

站点	计算机	可用硬盘空间	CPU	内存	视频卡
ORA					
	ORANGE2	1505	Intel Pentium II 处理器	97	ATI 3D RAGE PRO AGP (GT
	RED1	2242	Intel Pentium II 处理器	130	ATI 3D RAGE PRO AGP (GT
	RED2	1504	Intel Pentium II 处理器	130	ATI 3D RAGE PRO AGP (GT
PUR					
	PURPLE1	1331	Intel Pentium II 处理器	97	ATI 3D RAGE PRO AGP (GT
RED					
	ORANGE2	1505	Intel Pentium II 处理器	97	ATI 3D RAGE PRO AGP (GT
	RED1	2242	Intel Pentium II 处理器	130	ATI 3D RAGE PRO AGP (GT
	RED2	1504	Intel Pentium II 处理器	130	ATI 3D RAGE PRO AGP (GT

图 8.2：具有 Windows 2000 所需容量的计算机的 SMS 报告示例

许多单位的计算机内存少于 90M 或可用空间不到 1G，也有可能升级。没有理由认为一个没被 SMS 标识的视频卡就与不能兼容 Windows 2000。如果怀疑某些视频卡可能不兼容 Windows 2000，可以用它们的芯片种类值来替换空字符串。如果需要，可以添加额外标准。

示例查询如下：

```
SELECT DISTINCT SMS_G_System_LOGICAL_DISK.FreeSpace,
SMS_G_System_PROCESSOR.Name,
SMS_G_System_X86_PC_MEMORY.TotalPhysicalMemory,
SMS_G_System_VIDEO.AdapterChipType, SMS_R_System.Name,
SMS_R_System.SMSAssignedSites
FROM (((SMS_R_System LEFT JOIN SMS_G_System_PROCESSOR ON
SMS_R_System.ResourceId = SMS_G_System_PROCESSOR.ResourceID) LEFT JOIN
SMS_G_System_VIDEO ON SMS_R_System.ResourceId =
SMS_G_System_VIDEO.ResourceID) LEFT JOIN SMS_G_System_X86_PC_MEMORY ON
SMS_R_System.ResourceId = SMS_G_System_X86_PC_MEMORY.ResourceID) LEFT
JOIN SMS_G_System_LOGICAL_DISK ON SMS_R_System.ResourceId =
SMS_G_System_LOGICAL_DISK.ResourceID
WHERE (((SMS_G_System_LOGICAL_DISK.FreeSpace)>1000) AND
((SMS_G_System_X86_PC_MEMORY.TotalPhysicalMemory)>90000) AND
((SMS_G_System_VIDEO.AdapterChipType)<>'') AND
((SMS_G_System_LOGICAL_DISK.DeviceID)='C:')AND
((InStr(1,[SMS_G_System_PROCESSOR].[Name],"Pentium"))>0))
ORDER BY SMS_R_System.SMSAssignedSites;
```

您可以在 Microsoft Access 中执行这个查询。如果在 SMS Administrator 控制台使用这个查询，可以通过 SMS Query Extract Tool （SMS 查询提取工具）直接在 Microsoft Access 中使用。这个工具在 SMS 2.0 CD-ROM 的 Support 目录下，与 *Microsoft® BackOffice® Resource Kit 4.5.* 一并提供。请参见以前引用过的 Web 资源页，以获得有关带有或不带 SMS Query Extract Tool （SMS 查询提取工具）使用 Microsoft Access 来建立 SMS 报告的详尽论述。

使用产品兼容性子系统

SMS 的产品兼容性数据库通常用于将 SMS 软件清单报告的每台计算机的软件和一些有已知的 2000 年兼容性问题的软件进行比较。您还可以用这个子系统将软件与有已知的欧元兼容性问题的软件进行比较。这同样适用于 Windows 2000 兼容性 — 您可用 SMS 报告中的产品兼容性数据库突出显示那些有 Windows 2000

应用程序兼容性问题的计算机。

SMS 并不包含有 Windows 2000 兼容性问题的软件产品的列表。本书的“测试应用程序与 Windows 2000 的兼容性”一章可以帮助调查您单位有兼容性测试问题的应用程序分布在哪里。

用 Windows 2000 硬件或软件兼容性信息来扩充产品兼容性子系统

Microsoft® Systems Management Server Administrator's Guide 中的“确定产品兼容性”一章描述了 SMS 产品兼容性子系统。它包括添加新产品和基于产品兼容性类域的报告的步骤。

您只要用 SMS Administrator 控制台将新的条目添加至产品兼容性数据库即可。选择 **Product Compliance**（“产品兼容性”），然后从 **Action**（“操作”） 菜单里选择 **New**（“新建”）和 **Product Compliance**（“产品兼容性”）。显示 **Product Compliance Properties**（“产品兼容属性”）对话框。联机帮助描述了每个域。

注意：产品兼容性域必须与那些由 SMS 软件清单程序所查到的完全一致。用 **Browse**（“浏览”）按钮查找文件的特别示例能够保证文件名称和大小完全一致。产品名称、版本和语言域提供下拉式列表框，能让您选择 SMS 软件清单查到的准确值。

请特别注意 **Compliance Type**（“兼容类型”）和 **Compliance Level**（“兼容等级”）域。每个域包含一个下拉式列表框，列出了以前此域使用过的所有值。**Compliance Type**（“兼容类型”）的默认值为“Year 2000 Compliance”，但您可以键入任何值。您可能想用“Windows 2000 Compat.”。（值限制在 20 个字符以内）。

在您选择了某个兼容类型之前，**Compliance Level**（“兼容等级”）列表为空。当您选择了某个兼容类型，**Compliance Level**（“兼容等级”）列表将包括那个兼容类型以前用过的所有值。最初，没有值曾被使用过，所以列表为空。您可以键入任何值，如“Compatible”、“Incompatible”、“Compatible with minor issues”或“Compatible with major issues”。

提示：如果您想用和 2000 年兼容性一样的 Windows 2000 兼容等级，就暂时选择“Year 2000 Compliance”作为兼容类型，选择要用的兼容等级，然后复制到剪贴板。更改 Windows 2000 兼容等级并将复制的值粘贴到 **Compliance Level**（“兼容等级”）域。

用产品兼容性子系统报告

可以用 SMS 站点数据库报告 Windows 2000 兼容性。SMS_G_System_SoftwareProduct 类具备 SMS 软件清单程序发现的所有软件产品的属性。SoftwareProductCompliance 具备兼容数据库的属性。比较两个表中的相关属性可以发现是否每个软件产品都有兼容性问题。表 8.3 列出了您所需的属性。

表 8.3：产品兼容性数据

数据	SMS 软件清单属性	SMS 产品兼容性属性
文件名	FileName	FileName
文件大小	FileSize	FileSize
产品名称	ProductName	ResProdName
产品版本	ProductVersion	ResProdVer
产品语言	ProductLanguage	ResProdLangID

兼容类型	N/A	Type
兼容等级	N/A	Category

启用 SMS 产品兼容性子系统报告 Windows 2000 兼容性的最简单的方法是从现存的 2000 年兼容性查询中复制它的查询语句。然后，新建一个空的查询并将查询语句粘贴到这个新的查询。更改兼容类型值并输入其余的查询详细信息。比如，下面这个查询就基于标准的“ Y2K All Compliant Software by System in This Site and Its Subsites ”查询。此查询只作两处更改 — “ Year 2000 Compliance ”改为“ Windows 2000 Compat. ”。

示例查询如下：

```
SELECT DISTINCT sys.Name, compl.Category, compl.ProdName, compl.ProdVer,
compl.ProdCompany, compl.ProdLang, compl.URL, compl.Comment FROM
SMS_SoftwareProductCompliance as compl INNER JOIN
SMS_G_System_UnknownFile as unknownfile ON UPPER(unknownfile.FileName) =
UPPER(compl.FileName) AND unknownfile.FileSize = compl.FileSize AND
unknownfile.ProductId = 0 INNER JOIN SMS_R_System as sys ON
unknownfile.ResourceID = sys.ResourceID WHERE compl.Category !=
"Compliant" AND compl.Type = "Windows 2000 Compat."SELECT DISTINCT sys.Name,
compl.Category, compl.ProdName, compl.ProdVer,
compl.ProdCompany, compl.ProdLang, compl.URL, compl.Comment FROM
SMS_SoftwareProductCompliance as compl INNER JOIN
SMS_G_System_UnknownFile as unknownfile ON UPPER(unknownfile.FileName) =
UPPER(compl.FileName) AND unknownfile.FileSize = compl.FileSize AND
unknownfile.ProductId = 0 INNER JOIN SMS_R_System as sys ON
unknownfile.ResourceID = sys.ResourceID WHERE compl.Category !=
"Compliant" AND compl.Type = "Windows 2000 Compat."
AND (compl.ResProdLangID = prod.ProductLanguage OR compl.ResProdLangID =
65535) AND prod.ProductID = prodfile.ProductID
```

这个查询按站点返回列有不兼容软件的数据。可以使用这些数据创建 Microsoft Access 报告，如图 8.3 所示。

图 8.3：软件兼容性报告示例

这时，适当站点上的管理员会被警告，他们必须在其站点上解决应用程序兼容性问题。如果需要的话，计算

机名称和其它详细信息很容易包含在报告中。查询结果也可用作 SMS 集，可以将 SMS 程序包通知它，以升级或删除应用程序。

分析和使用收集的数据

人们通常分析报告中的数据来回答如下一些问题：“ 将客户计算机升级到 Windows 2000 需要多少钱？ ”或“ 我需要向成本中心申请多少资金？ ”但是，当涉及许多站点和计算机时，进行手工分析将是一件极其繁重的工作。因此，将数据提取到工具（可以用该工具进行分析）中也许更为可取。你可以使用 SMS Query Extract Tool （SMS 查询提取工具）方便地将有助于部署 Windows 2000 的数据提取到诸如 Microsoft Excel 或 Microsoft Access 这样的工具中。*Microsoft® Systems Management Server Administrator's Guide*（*Microsoft® BackOffice® Resource Kit 4.5* 的一部分）中的“ SMS 2.0 报告选项 ” 一章对此进行了详细描述。

您的最终目标是部署 Windows 2000，而您可以使用 SMS 收集的数据来自动执行这个程序。为‘ Our Windows 2000–Ready PCs ”这类报告提供数据的同样查询也可以用作在 Windows 2000 公告的 SMS 数据库中计算机收集的基础。

同样，就象 SMS 产品兼容性子系统显现的那样，为了兼容 Windows 2000 ，某些计算机的软件需要升级。收集的软件清单也可以用来定位那些需要进行合理升级（可通过 SMS 进行）的计算机 。

您可能希望用 SMS 以外的工具来安装 Windows 2000 或者升级应用程序。这些工具也需要定位一系列计算机，您同样可以用 SMS 数据达到这个目的。数据可以用以前讨论过的技术提取，而且无论采取哪种技术，数据可以输入到别的工具里。

有关使用 SMS 部署 Windows 2000 的详细信息，请参见本书的“ 使用 Systems Management Server 部署 Windows 2000 ”。部署 Windows 2000 兼容应用程序可以用非常类似的方法进行。

监视网络

准备部署 Windows 2000 的一个非常重要的方面是了解您的网络。您需要回答这样的问题：

- 哪个网络链接和网段的容量有限？
- 使用哪种协议？
- 动态主机配置协议 (DHCP)、 Windows Internet 命名服务 (WINS) 和其它类似服务器在哪里？

传送 Windows 2000 源文件至远程站点需占用大量的网络容量。以共享方式安装 Windows 2000 需要更多的容量，局域网络必须有此容量。核实使用了哪些协议以及网络服务器的位置，有助于确保您的规划包括所有相关细节。

SMS 包含 Network Monitor （网络监视器）和相关功能，有助于分析网络和回答这些类似的问题。Network Monitor （网络监视器）可以显示每个网段的活动层，如图 8.4 所示。Network Monitor （网络监视器）也能捕获网络数据包。您可以审阅这些数据包，查看正在使用哪种协议以及哪些计算机正在提供服务。Network Monitor （网络监视器）包含一种叫做 Network Monitor Experts （网络监视器专家）的功能，它甚至还产生一个表格，列出使用的协议以及每个协议使用的帧和字节数的百分比。

图 8.4：SMS Network Monitor （网络监视器）

可以配置 Network Monitor Control Tool （网络监视器工具）来持续监视网络活动，以发现未经授权的 DHCP

和 WINS 服务器。您向工具提供您了解的 DHCP 和 WINS 服务器地址，它就会显示任何发现数据包的其它 DHCP 和 WINS 服务器的地址。

Systems Management Server Administrator's Guide 中的“使用 SMS 进行网络维护”一章详细描述了 Network Monitor （网络监视器）的使用方法。

备注：Windows 2000 包含 Network Monitor（网络监视器）的一个版本。但是，那个 Network Monitor （网络监视器）版本只能监视进出它所在的计算机的通信，包括广播。而 SMS 版本的 Network Monitor （网络监视器）监视它负责的网段上的所有通信。SMS 2.0 版本的 Network Monitor （网络监视器）还包括其它增强功能，如 Network Monitor Experts （网络监视器专家）。

确保应用程序兼容性

SMS 能在许多方面帮助您部署 Windows 2000。SMS 的一个重要功能是增强 Windows 2000 兼容性应用程序的使用。

可使用 SMS 定位需进行软件升级的计算机，并把软件传送到那些计算机。可以自动升级或用户输入信息升级。升级的时间可由 SMS 管理员安排，用户可以调整日程使升级工作在用户开会或方便的时候进行。

升级工作还可在授予 SMS 的安全权限下进行，这样用户无需对正在使用的计算机具有哪怕是临时的高级权限。使用 SMS 软件分布的一个重要的优点是升级能够返回状态消息。因此，可以轻易地报告升级进程。

SMS 可通过禁止用户运行不兼容的应用程序来确保应用程序与 Windows 2000 的兼容性。用户可能希望使用他们熟悉的应用程序和版本，而忽略升级应用程序中的公司标准或新功能的带来的好处。所以有必要强化执行应用程序标准。本书“测试应用程序与 Windows 2000 的兼容性”一章论述的方法能用来确定哪些应用程序与 Windows 2000 不兼容。

兼容性确定后，可定义这些应用程序以进行 SMS 软件测试，许可证数量可设为 0。这样就可禁止用户使用旧版本软件了。当然这种方法最好与有效的沟通和训练计划共同使用，让用户理解必须使用被认可的应用程序以便于迁移。

备注 SMS 软件测试可以两种模式进行：联机或脱机。联机模式下，每次程序被调用时客户机和服务器一起检查。要共享许可证，必须使用这种模式。脱机模式下，客户机记录所有程序调用，但以不频繁间隔上载数据。这将大大降低网络、客户机和服务器的负载。脱机模式下，无法共享许可证，但通过设定可共享许可证数量为 0 和不可用日程安排为每天 24 小时，程序就被禁止使用。许可证执行不能建立在 Windows NT 用户组成员身份基础上。

有关软件分发，包括生产、分布、广告和监视 SMS 软件分发数据包的过程，请参见本书的“使用 Systems Management Server 部署 Windows 2000”。请参见 *Systems Management Server Administrator's Guide*，以获得有关 SMS 软件发布和 SMS 软件测试的一般性讨论。

网络分析规划任务列表

使用表 8.4 确保采取所有必要的步骤准备网络基础结构。

表 8.4：网络分析规划任务列表

任务	所在章节

收集硬件清单	评估硬件当前状态
收集软件清单	评估软件当前状态
收集软件使用数据	评估软件当前状态
报告收集的数据	报告收集的数据
分析收集的数据	分析和使用收集的数据
用兼容数据库分析收集的数据	报告收集的数据
监视网络	监视网络

其它资源

- 有关 SMS 的规划和使用的详细信息，请参见包含在 SMS 中的 *Microsoft® Systems Management Server Administrator's Guide*。
- 有关 SMS 产品的详细信息，请参见 Web 资源页的 Microsoft Systems Management Server 链接，地址是： http://windows.microsoft.com/windows2000/reskit/webresources。
- 有关如何基于 SMS 收集的收据撰写报告的信息，请参见 Web 资源页的 Microsoft Systems Management Server Technical Details 链接，地址是： http://windows.microsoft.com/windows2000/reskit/webresources。
- 有关 SMS 的高级信息，请参见 *Microsoft® BackOffice® Resource Kit 4.5* 中的 *Microsoft® Systems Management Server Resource Guide*。

第 9 章 - 设计 Active Directory 结构

Microsoft® Windows® 2000 Server 包括名为 Active Directory™. 的目录服务。本章所介绍的 Active Directory 概念、体系结构元素和功能，能帮助本单位的 IT 体系结构设计人员和策略规划人员创建设计文档，这些文档对于成功部署 Microsoft® Windows® 2000 Active Directory 必不可少。

在阅读本章之前，详细了解本单位的 IT 管理组、管理层次结构和网络拓扑是很重要的。了解这些情况可帮助您将本章的规划指导方针应用到您自己的具体环境中。

本章内容

Active Directory 概述
Active Directory 规划
制定目录林规划
制定域规划
制定部门规划
制定站点拓扑规划
设计 Active Directory 结构规划任务列表

本章目标

本章将帮助您创建下列规划文档：

- 目录林规划
- 每个目录林的域规划
- 每个域的部门 (OU) 规划
- 每个目录林的站点拓扑规划

资源工具包中的相关信息

- 有关将域迁移到 Windows 2000 的详细信息，参见本书中的“确定域迁移策略”。
- 有关 Windows 2000 安全标准（例如 Kerberos 协议）的详细信息，参见本书中的“规划分布式安全性”。
- 有关高级网络的详细信息，参见本书中的“确定网络连接策略”。
- 有关 Microsoft® IntelliMirror™ 或组策略的详细信息，参见本书中的“应用更改与配置管理”。
- 有关 Active Directory 的详细技术信息，参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide.*
- 有关域名系统 (DNS) 的详细信息，参见 *Microsoft® Windows® 2000 Server Resource Kit TCP/IP Core Networking Guide* 中的 "Introduction to DNS" 和 "Windows 2000 DNS"。

Active Directory 概述

Active Directory 具有许多作用，包括从充当分布式安全性骨干到提供服务发布框架等。Active Directory 提供一种集中服务，以便管理员组织网络资源、管理用户、计算机和应用程序，并保护 Intranet 和 Internet 网

络访问的安全。

由于有越来越多的分布式应用程序利用 Active Directory，可以无须实现和管理应用程序专用目录服务。结果，可以节省管理成本和硬件成本。

注意 可以在部署 Active Directory 之前、同时或之后部署 Windows 2000 Server 和 Microsoft® Windows® 2000 Professional。不必首先部署 Active Directory。可以立即升级成员服务器和客户计算机，利用 Windows 2000 的许多新功能。有关升级成员服务器的详细信息，参见本书中的“升级和安装成员服务器”。

Active Directory 主要功能

Windows 2000 Active Directory 的功能为网络带来许多优点，包括：

安全性

Active Directory 为多种新安全功能提供基础结构。使用相互身份验证，客户机便可以在传送敏感数据之前验证服务器身份。使用公钥安全支持，用户可以用智能卡代替密码进行登录。

管理简便且灵活

Active Directory 中的对象具有按属性的访问控制，因而可进行细粒度的管理委派。管理委派使您更高效地分散单位的管理责任，从而减少必须具有域范围内控制的用户数。

可扩展性

Active Directory 将域名系统 (DNS) 用作定位机制。DNS 是层次化、分布式和高扩展性的名称空间，用于在 Internet 上将计算机和服务名称解析为传输控制协议 / Internet 协议 (TCP/IP) 地址。

目录用域来存储信息，域是能让您在速度和可靠性各不相同的大型网络上分发目录的分区。目录采用了数据库技术，而且经测试，可以接受几百万个对象（用户、组、计算机、共享文件夹、打印机，等等）。可伸缩定位、分区和可伸缩存储量的这种组合能确保目录随本单位的成长而相应扩大。

高可用性

采用单一主控复制的传统目录的查询操作具有高可用性，但更新操作却没有。而采用多主控复制的 Active Directory，查询操作和更新操作都具有高可用性。

可延伸性

架构包含可存在于目录服务中的每个对象类别的定义，是可延伸的。这就允许管理员和软件开发人员可以根据其需要来量身定做目录。

开放的标准支持

Active Directory 建立在基于标准的协议上，例如：

- DNS，用于定位运行 Active Directory 的服务器。
- Lightweight Directory Access Protocol (LDAP)，用作查询和更新协议。
- Kerberos 协议，用于登录和身份验证。

这种对开放标准的支持使得将众多软件（例如基于 LDAP 的通讯簿客户软件）同 Active Directory 一起使用成为可能。

简单程序访问

可以从许多编程平台上访问 Active Directory 服务接口 (ADSI)，包括 Visual Basic Script 等脚本语言平台。使用 ADSI，系统管理员和软件开发人员可以迅速编制功能强大的支持目录的应用程序。举一个支持目录的应用程序的例子，如从目录中读取数据或配置信息的应用程序。

为新技术提供基础

除了上述基本优点之外，Active Directory 还将在 Windows 2000 部署中起重要作用，因为它是其它新技术和功能的实现基础，例如：

IntelliMirror

Windows 2000 提供许多更改和配置管理技术。IntelliMirror 和远程操作系统安装管理软件能帮助您减少用在客户管理和支持上的工作量和成本。有关实现这些技术的详细信息，参见本书中的“应用更改与配置管理”与“定义客户管理与配置标准”。

目录合并

Active Directory 具有可扩展性和可延伸性，是网络上使用独立内部目录的应用程序的理想合并点。例如，可以：

- 进行完全目录合并，这样 Microsoft® Exchange Server 等产品可以摆脱目录组件，单独依靠 Active Directory 进行管理和操作。
- 合并管理，这样可在 Active Directory 中管理目录信息，并用目录同步法来使远程目录保持最新状态。
- 合并现有的 Microsoft® Windows NT® 域，这样就有可能减少网络上需要管理的对象和硬件的总数。

高级网络

Internet 协议安全性 (IPSec)、网络服务质量功能和新的远程访问功能是 Active Directory 赋予的高级网络功能的例子。

为 Active Directory 制定规划

在规划和部署企业级 Active Directory 时，您是在定义本单位网络基础结构中的重要部分。在该规划中，应建立一套最能反映本单位情况的结构。创建的结构将决定：

- 目录的可用性和容错能力。
- 目录客户机和服务器的网络使用特征。
- 管理目录内容的效率。
- 用户查看目录和与目录互动的方式。
- 目录结构随本单位的发展而发展的能力。

考虑周全的 Active Directory 规划对于性能价格比合理的部署至关重要。在规划阶段花一些时间，有助于您避免将来在已搭建的结构上花费太多时间与金钱。

要制定目录结构规划，按本章提供的规划步骤顺序进行。在制定规划时：

- 学习影响结构规划的 Active Directory 关键概念，对建议的规划步骤作必要的调整，以最适合本单位的需要。
- 确定本单位中应参与结构规划的人员。
- 了解现有的业务操作需要做哪些改变或发展才能充分利用 Active Directory。
- 了解您建立的结构的灵活性，了解在您的选择中，哪些可以在将来容易改变，哪些难于改变。

图 9.1 说明设计 Active Directory 结构的主要步骤。本章将对这些步骤中的每个步骤作详细介绍。

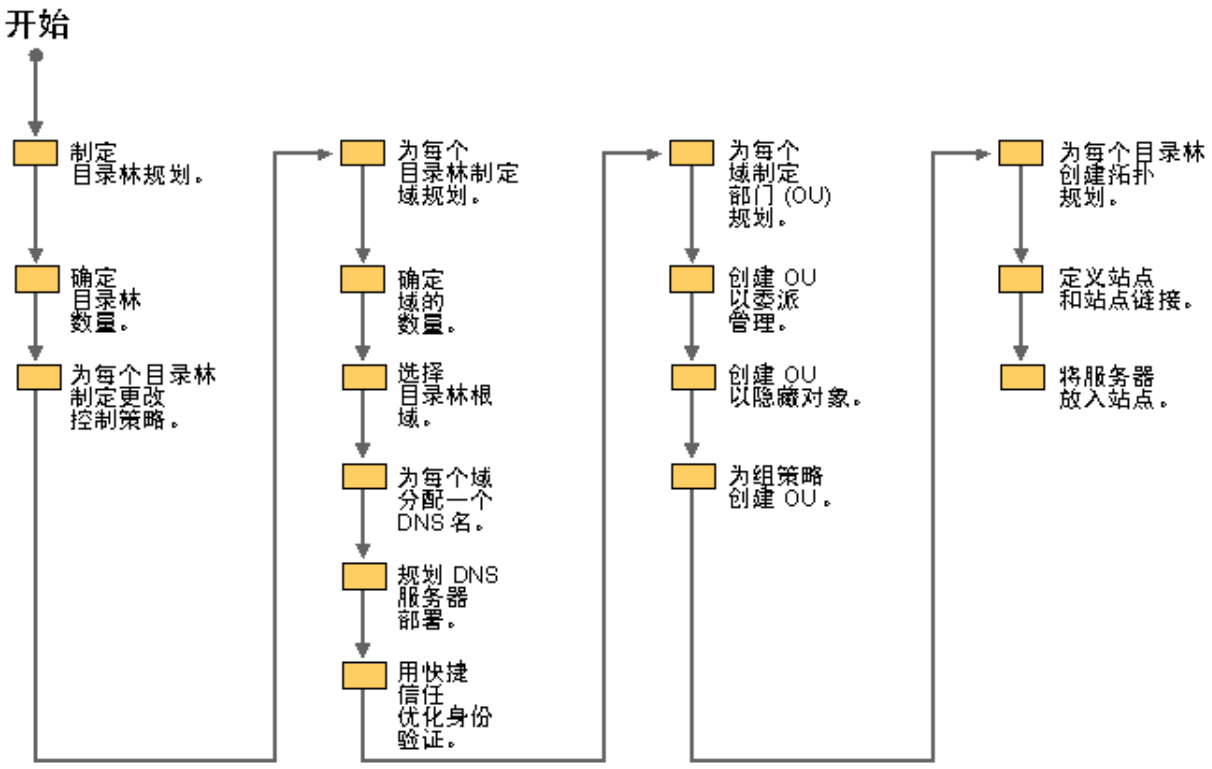


图 9.1 Active Directory 结构设计过程

总的设计原则

在做 Active Directory 规划时，用以下设计原则来指导您的决策过程：

简单是最好的投资。

简单的结构易于说明、维护和调试。尽管增加某些复杂结构可以增值，但要衡量一下逐步的增值和将来的潜在维护费用之间的关系。例如，最大程度地优化查询和复制通信可能需要复杂的站点拓扑。但是，复杂的站点拓扑比简单的站点拓扑维护起来更难。在确定复杂的结构之前一定要权衡一下功能增强与复杂性增大之间的利弊。

您建立的每一样东西在其整个寿命期内都需要一些维护。如果没有明确理由建立一种结构，最后它长期耗费

的金钱将多于任何增值。明确您建立的任何结构的合理性。

您的业务和单位会不断变化。

任何单位内的正常变化，从人员流动到整个企业的重组或购并，都将影响 Active Directory 结构。在设计结构时，应考虑这些潜在的变化对最终用户和管理员同目录的交互方式所带来的影响。例如，应考虑最近一次重大业务重组对您设计的结构可能会有什么影响。试想一下，如果新加一个位置或代表处需要做哪些必要的修改？这些修改要求对 Active Directory 做昂贵的大的变动吗？确保您的设计足够通用和足够灵活，以适应经常的大的变动。

理想设计的目标。

在第一阶段设计时，设计出您认为理想的结构，即使它不能反映当前域或目录基础结构。了解什么是理想的东西将是有帮助和可行的，哪怕它目前还不能实现。有关将网络迁移到理想规划所涉及成本的详细信息，参见本书中的“ 确定域迁移策略 ”。将这些成本和理想规划的长期节省对比一下，然后再适当修改设计。

研究设计替代的方案。

在每次设计时提供一种以上方案。将某种设计与其它设计思想进行比较，其优点就会变得更加明显。将所有设计的最佳之处集中到您将要实现的规划中。

集中 Active Directory 结构规划

Active Directory 结构由四个基本组件组成：目录林、域、部门和站点。Active Directory 结构规划的目标是为结构中的每个组件制定规划文档，并在这个过程中收集重要的决定和正当理由。然后，这些规划文档就会作为下一个规划任务和迁移的起点。组成 Active Directory 结构规划的四个规划文档为：

- 目录林规划
- 每个目录林的域规划
- 每个域的部门 (OU) 规划
- 每个目录林的站点拓扑规划

制定目录林规划

目录林是 Active Directory 域的集合。目录林有两种主要用途：简化用户与目录的交互过程和简化对多个域的管理。目录林具有以下主要特征：

单一架构

Active Directory 架构定义对象类别和可以在目录中创建的对象类别属性。对象类别定义可以在目录中创建的对象的类型。架构充当命名环境，可复制到目录林中的各个域控制器。架构管理员安全组完全控制架构。

单一配置容器

Active Directory 配置容器是命名环境，可复制到目录林中的每个域控制器。支持目录的应用程序在配置容器中存储应用于整个目录林的信息。例如，Active Directory 将物理网络的有关信息存储在配置容器中，并用这些信息来指导创建域控制器之间的复制连接。企业管理员安全组完全控制配置容器。

在目录林的所有域间共享单一而且一致的配置，就不再需要对域进行逐个配置。

完全信任

Active Directory 在目录林的域之间自动创建可传递的双向信任关系。来自任何域的用户和组都能被目录林中的任何计算机识别，并包括在组或访问控制列表 (ACL) 中。

完全信任使得在 Windows 2000 中管理多个域更加简单。在以前的 Windows NT 版本中，部署域的流行模式为多母版域模式。在这种模式中，主要包含用户帐户的域称为主用户域，而主要包含计算机帐户和资源的域则称为资源域。常见部署由少数主用户域构成，每个主用户域都受到大量资源域的信任。在部署中增加一个新域要求建立多个信任。采用 Windows 2000 Active Directory，在您将一个域添加到目录林时，此域会自动配置为双向可传递信任。这可以避免建立与同一个目录林中的域的其它信任。

单一全局编录

全局编录包含来自目录林中每个域的每个对象的一个副本，但只包含每个对象的一个属性选集。全局编录能使您在整个目录林内进行快速、高效的搜索。

全局编录使目录林中的目录结构对最终用户透明。将全局编录用作搜索范围使得在目录中查找对象更加简单。采用全局编录和用户主要名称使得登录更加简单，如下所述：

用户搜索全局编录 在目录搜索用户界面中，当选择一个搜索范围时，将全局编录抽象为“完整目录”。用户没有目录林结构的预备知识便可以搜索目录林。拥有单一而一致的搜索界面就无须对用户进行有关目录结构的培训，并允许管理员更改目录林中的结构，而不影响用户与目录的交互方式。

用户通过用户主要名称登录 用户主要名称 (UPN) 是一个类似于电子邮件的名称，它唯一地代表一个用户。UPN 由两个部分组成，用户标识部分和域名部分。这两个部分由 @ 符号分隔，形如<用户>@<DNS 域名>，例如 liz@noam.reskit.com。给每个用户都会自动指派一个默认 UPN，其中<用户>部分与用户的登录名相同，而该名称的<DNS 域名>部分是用户帐户所在 Active Directory 域的 DNS 名。在用 UPN 登录时，用户不再需要从登录对话框上的列表中选择域。

可以将 UPN 设置为任意值。例如，即使 Liz 的帐户在 noam.reskit.com 域中，也可以将其 UPN 设置为 liz@reskit.com。当用户登录时，查找要验证的用户帐户的方式为，在全局编录中搜索具有匹配 UPN 值的用户帐户。通过使 UPN 值独立于域名，管理员可以在域之间移动用户帐户，而不会更改 UPN 值，并使得跨域移动对用户更加透明。

目录林规划过程

为单位制定目录林规划的主要步骤如下：

- 确定网络的目录林数量。
- 制定目录林更改控制策略。
- 了解进行部署后，更改对目录林规划的影响。

在制定目录林规划时，可能需要咨询：

- 负责用户帐户、组和计算机的现任域管理员。
- 网络安全组。

确定网络的目录林数量

开始规划目录林模式时，从单一目录林着手。在很多情况下，单一目录林就足够了。但是，如果您决定创建其它的目录林，确保您具备有效的技术理由。

建立单一目录林环境

单一目录林环境易于建立和维护。所有的用户都通过全局编录看到单一的目录，而无需知道任何目录结构。当将新域添加到目录林时，不要求其它的信任配置。只需应用一次配置更改即可影响所有域。

建立多目录林环境

如果网络管理分布在多个自治部分之间，则有必要创建一个以上的目录林。

由于目录林具有共享元素（例如架构），因此目录林中的所有参与者必须同意这些共享元素的内容和管理。合作伙伴与大企业等单位可能没有一个集中的实体来启动此过程。在合资企业等短期单位中，期望各个单位的管理员在目录林管理上进行合作是不现实的。

如果各个单位符合下列情况，就必须建立一个以上的目录林：

不互相信任管理员。目录林中每个对象有一个代表驻留在全局编录。被委派了对象创建能力的管理员有意或无意地建立一种“拒绝服务”条件是有可能的。可以迅速创建或删除对象以建立此条件，从而为全局编录带来大量复制。过多的复制会浪费网络带宽并减慢全局编录服务器的速度，因为这些服务器要花时间来处理复制。

不同意某种目录林更改策略。架构更改、配置更改和向目录林新加域会影响到整个目录林。目录林中的每个单位都必须同意实现这些更改的过程，同意架构管理员和企业管理员组的成员身份。如果单位不同意一个公共策略，它们就不能共享相同的目录林。本章后面部分将讨论目录林更改策略。

希望限制信任关系范围。目录林中的每个域都信任该目录林中的所有其它域。可以将目录林中的每个用户包括进某个组成员关系中，或使其出现在目录林中任何计算机的访问控制列表上。如果希望防止将特定资源的访问权限授予特定用户，则必须让这些用户驻留在与资源不同的目录林中。如果必要，可以用显式信任关系来允许这些用户获得访问特定域中的资源的权限。

增加目录林的成本增加

每建立一个目录林都会耗费一定的管理开销，例如：

- 每增加一个目录林必须至少包含一个域。这可能要求您所拥有的域必须多于您最初规划的域。建立和维护域都是有固定成本的。本章的后面部分将给出这些成本的详细信息。
- 必须对每个目录林的整个目录林范围的组件（例如，架构与配置容器元素及其相关管理组成员）进行单独管理，尽管它们实质上是一样的。

为了让某个目录林中的用户使用其它目录林中的资源，需要下列额外配置：

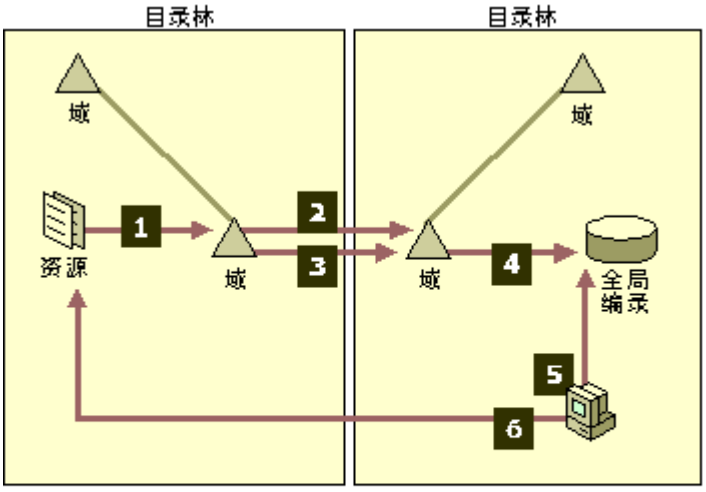
- 要让某个目录林中的用户访问另一个目录林中的资源，必须在这两个域之间建立和维护显式信任关系。不同目录林中的域之间的显式信任关系是单向而且是不可传递的。不建立信任关系，就不能授权某个目录林中的用户访问另一个目录林中的对象的权限。

  默认情况下，一个目录林中的用户仅知道本目录林的全局编录中的对象。要查找不同目录林中的对

象，用户必须向其目录林之外的域进行外部查询。或者，管理员可以将其它域中的数据导入用户所在的目录林。这会增加成本，因为：

- 用户必须接受培训，了解目录结构，以便知道在全局编录查询失败时，应该将查询转到何处。
- 如果从其它目录林中的域导入数据，必须放入一个进程，以便源域中的数据更改时，使导入的数据保持最新状态。

图 9.2 是一个跨目录林配置例子，其中一个目录林中的用户需要访问另一个目录林中的已发布资源。建立一个显式单向信任关系，以便用户可以获得访问资源的权限。目录中的资源代表复制到用户域中，此资源代表出现在全局编录中。



1. 在目录服务中发布的资源。
2. 管理员配置外部单向信任关系。
3. 管理员将对象导入目录林。
4. 将对象复制到全局编录。
5. 用户通过查询全局编录查找对象。
6. 用户访问资源。

图 9.2 跨目录林资源访问其它配置

在某个目录林中可用的某些功能在跨目录林时是不可用的，例如：

- 如果用户帐户在与用于登录的计算机的不同的目录林上，则只能使用默认 UPN。默认 UPN 是必需的，因为计算机目录林中的域控制器不能在全局编录中查找到具有匹配 UPN 的用户帐户。用户帐户出现在另一个目录林的全局编录中。然后，处理登录的域控制器必须用 UPN 的 <DNS 域名> 部分来尝试查找域控制器以验证用户身份。
- 用智能卡进行的登录依赖用户主要名称。对于用智能卡来工作的跨目录林登录过程，必须使用默认 UPN。
- 可以在同一目录林的域间移动安全主管，但在不同目录林的域间则必须复制它们。对最终用户来说，在域间进行复制不如在域之间移动用户那样透明。有关复制的详细信息，参见本书中的“确定域迁移策略”。

在确定需要的目录林数目时，记住对用户重要的东西未必与对管理员重要的东西一样。但是，用户会失去多目录林方案的大多数益处。例如，有些单位将其网络管理外包给几个不同的承包商。通常，承包商取得的报酬是根据网络性能而定的，并且他们的首要责任是维护网络稳定。一个承包商可能不希望另一个承包商影响他所控制的计算机，并有独立的目录林才能化解这一挑战。但是，独立的目录林可能对用户不利，因为他们

不再具有单一而且一致的目录视图。在这些情况下，尽量不要建立独立目录林来解决管理界限问题。

在让所有用户拥有一致的目录视图并不重要的情况下，才可能适合拥有多个目录林。例如，让我们看看 Internet 服务提供商 (ISP) 这样的公司，它有代表几家公司主持 Active Directory。不同客户公司中的用户没有理由共享一致的目录视图。此外，公司间也没有理由拥有可传递的信任关系。在这种情况下，维护独立的目录林是有帮助和合适的。

制定目录林改变控制策略

建立的每个目录林都应当有一个相关的目录林更改控制策略，它是目录林规划文档的组成部分。您将用此策略来指导会影响整个目录林的更改。您无需在继续下去前确定各个过程，但了解其从属关系是重要的。策略应包括目录林中每个共享元素的有关信息。

架构改变策略

架构管理员组完全控制目录林架构。架构改变策略应包括：

- 本单位中控制架构管理员组的小组名称。
- 架构管理员组的起始成员身份。
- 用于请求和评估架构改变的指导方针和过程。

有关 Active Directory 架构的详细信息，参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide*.

配置改变策略

企业管理员组完全控制在整个目录林中复制的配置容器。配置改变策略应包括：

- 本单位中控制企业管理员组的小组名称。
- 企业管理员组的起始成员身份。
- 在目录林中建立新域的指导方针和过程。
- 修改目录林站点拓扑的指导方针和过程。（本章后面的“制定站点拓扑规划”会讨论站点拓扑。）

在部署后改变目录林规划

创建域时，可以将其加入现有目录林。可以通过将基于 Windows 2000 的服务器升级为 Active Directory 域控制器，或将 Microsoft® Windows NT® 3.51 版或 Microsoft® Windows NT® 4.0 版主域控制器升级到 Windows 2000 来创建域。

	关键决策点 不能通过一步操作合并两个目录林，也不能通过一步操作来在目录林之间移动域。设计目录林策略，以便本单位发展时，只需进行最少量的结构调整是很重要的。

可以在目录林间移动各个对象。移动对象的类型决定用来移动它的特殊工具。用 LDAP 数据交换格式 (LDIFDE.EXE) 命令行工具可以实现大多数大宗导入和导出，用ClonePrincipal 工具可以复制安全主管。有关这些工具的详细信息，参见 *Windows 2000 Resource Kit* 所带 CD 上的“工具帮助”。

制定域规划

以下是 Windows 2000 域的一些重要特征，着手制定域结构规划时，您需要予以考虑：

目录林分区

Active Directory 目录林是分布式数据库，其中的数据库分区由域定义。分布式数据库是由分散在许多计算机上的许多局部数据库组成的数据库，而不是某一台计算机上的单一数据库。将数据库分成更小的组成部分，把这些组成部分放在最合适的位置，可允许将大型数据库有效地分布到大型网络上。

域控制器服务器提供的服务

与在 Windows NT 4.0 中一样，运行 Windows 2000 的主持域数据库的服务器称为域控制器。一个域控制器只能主持一个域。可以更改某个域中任何域控制器上的域内对象。特定目录林中的所有域控制器还主持目录林配置和架构容器的副本。

身份验证单位

每个域数据库都包含安全主管对象，例如用户、组和计算机。安全主管对象是专用的，因此可以允许或拒绝它们访问网络上的资源。安全主管对象必须由它们所在的域的域控制器来进行身份验证。对象访问资源之前接受验证以验证其身份。

管理策略和组策略的分界

每个域都有一个域管理员组。域管理员完全控制域中的每个对象。这些管理权限仅在域内有效而不适用于其它域。

与某个域相关的组策略不能自动沿用到目录林中的其它域。要某个域的组策略与另一个域关联，必须让它进行显式链接。

独特域用户帐户安全策略

少数应用于域用户帐户的安全策略只能根据每个域的情况来设置：

- 密码策略。确定用户设置密码时必须满足的规则，例如密码长度。
- 帐户锁定策略。定义入侵检测和帐户停用规则。
- Kerberos 票据策略。确定 Kerberos 票据的寿命。Kerberos 票据是在登录过程中获得的，用于网络身份验证。特定的票据仅在策略中指定的寿命期内有效。票据到期时，系统自动尝试获取新票据。

有关域用户帐户安全策略的详细信息，参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide*.

DNS 域名

域由 DNS 名标识。DNS 用于定位给定域的域控制器服务器。DNS 名是分层次的，Active Directory 域的 DNS 名表示它在目录林层次结构中的位置。例如，reskit.com 可能是某个域的名称。名为 eu.reskit.com 的域可以是目录林层次结构中的 reskit.com 的子域。

域规划过程

您的域规划将决定网络上的目录的可用性、客户的查询通信特征和域控制器的复制通信特征。

您创建的目录林将包含一个或多个域。为目录林制定域规划的步骤为：

- 确定每个目录林中域的数量。
- 选择目录林根域。
- 为每个域指派一个 DNS 名以创建域层次结构。
- 规划 DNS 服务器部署。
- 用快捷信任关系优化身份验证。
- 了解进行部署后，更改对目录林规划的影响。

为每个目录林创建域规划时，您很可能需要咨询下列各组：

- 负责用户帐户、组和计算机的现任域管理员
- 管理和监控物理网络的小组
- 管理网络 DNS 服务的小组
- 安全小组

确定每个目录林中域的数量

要确定每个目录林的域的数目，开始时仅考虑一个域，即使您目前有一个以上的 Windows NT 4.0 域。然后，为每增加一个域提供详细理由。您创建的每个域会因需要其它的管理开销而带来一定程度的成本上升。因此，确保添加到目录林中的域都是有益的。

创建的域为何改变

在以前版本的 Windows NT Server 中导致多域环境创建的某些因素不再适用于 Active Directory 和 Windows 2000。这些因素是：

安全帐户管理器 (SAM) 大小限制 在以前版本的 Microsoft® Windows NT® Server 中，SAM 数据库有一个限制，即：每个域只能有大约 40,000 个对象。Active Directory 可以轻易扩展到每个域几百万个对象的容量。完全没必要为处理更多的对象而创建更多的域。

主域控制器 (PDC) 可用性要求 在以前版本的 Windows NT Server 中，只有 PDC 一个域控制器可以接受对域数据库的更新。在一个有大型网络的单位中，这一限制给确保 PDC 的高可用性带来了困难，因为网络故障会妨碍网络上某个部分的管理员对域进行更新。为了满足可用性要求，您需要创建更多的域，以便在整个网络上分布 PDC 服务器。在 Windows 2000 中，这些工作不再必需，因为所有的 Active Directory 域控制器都能接受更新。

域内的管理委派受限 在以前版本的 Windows NT Server 中，您委派管理的方式是使用帐户操作员组等内置本地组，或创建多个域并有不同的域管理员集合。例如，要委派对某个用户集合的管理，可以新建一个用户域。要委派对文件服务器或打印服务器等资源服务器的管理，可以创建资源域。在 Windows 2000，用部门 (OU) 在域内进行管理委派是可能的。OU 是一个容器，用于将域内的对象组织到逻辑管理子组中。OU 比域更加易于创建、删除、移动和修改，而且它们更适合委派作业。

有关用 OU 委派管理的详细信息，参见本章后面的“制定部门规划”。

何时创建多个域

创建更多的域的三种可能的原因是：

- 保留现有 Windows NT 域。
- 管理分区。
- 物理分区。

保留现有 Windows NT 域

如果您现在已有 Windows NT 域，您可能宁愿保留其原样，而不愿将其合并到更少量的 Active Directory 域中。如果决定保留或合并域，一定将这些成本和拥有更少的域的长远利益权衡一下。本书中“确定域迁移策略”一章讨论了与域合并有关的成本。如果您是第一次进行域设计，建议您计划采用尽可能少的域，并且在阅读那一章后重新评估该规划。

管理分区

因本单位的管理和策略要求（如下文所述）的不同，也有可能必须采用更多的域。

独特域用户安全策略要求 您可能希望网络上的某个用户集合遵守某个域用户安全策略，这个安全策略与应用于其他用户团体的安全策略不同。例如，您可能希望管理员拥有比网络上普通用户的密码策略更安全的密码策略，例如更短的密码更改间隔。为此，必须将这些用户放在单独的域中。

需要有自治管理监督的部门 特殊域中的域管理员组成员完全控制该域中的所有对象。如果本单位中有一个子部门不允许外部管理员控制其对象，将这些对象放在单独的域中。例如，出于法律原因，让某单位中的一个处理高度敏感项目的子部门接受一个更高级的 IT 组的域监督可能不够明智。记住目录林中的所有域都必须共享配置和架构容器。

物理分区

进行物理分区涉及取出您在某个目录林中拥有的域，然后将其分成更多更小的域。拥有更多更小的域允许您仅将对象复制到最有关的位置，从而优化复制通信。例如，在包含单一域的目录林中，目录林中的每个对象都复制到该目录林中的每个域控制器中。这可能会导致将对象复制到很少用到它们的位置，这不是一种有效利用带宽的方法。例如，始终在总部登录的用户不需要将其用户帐户复制到分支机构。为总部位置创建独立的域，而且不将此域复制到分支机构，可以避免复制通信。

注意 如果已部署 Windows NT 4.0 域，您可能对现有的物理分区满意。从清洁页再次查看分区可以鉴别出可进行域合并的区域。如果已决定升级现有 Windows NT 4.0 域且不做任何合并，您可以跳过分区讨论。

要确定是否对目录林进行分区以及如何分区，您应当：

- 绘制网络拓扑图。
- 根据可用性要求将域控制器放进网络。
- 根据域控制器之间的复制通信分区目录林。

绘制网络拓扑图

从绘制基本的网络拓扑布局图着手工作。在规划过程后期，在规划站点拓扑时将更多的信息添加到此布局图。要绘制拓扑布局图：

- 绘制站点集合图。

  站点是一个速度快、连接可靠的网络。局域网 (LAN) 或通过高速骨干网连接起来的 LAN 集合可视为站点。在网络布局图上画出各个站点，并标明每个站点的大约用户数。

- 用站点链接将站点连接起来。

  站点链接是连接两个站点的较慢的或不太可靠的链接。连接两个快速网络的广域网 (WAN) 是站点链接例子。建议您将速度比 LAN 慢的链接都视为慢链接。在拓扑布局图中，表明每个站点是如何通过站点链接连接到其它站点的。

  对于每个站点链接，记录下：

  - 链接速度和当前使用程度
  - 链接是否根据使用程度收费
  - 该链接是否出现过不稳定的情况
  - 是否只能间断地使用此链接

- 仅用 SMTP 连接来标记站点。

  如果您有一个与网络的其余部分之间没有物理连接，但可以通过简单邮件传输协议(SMTP) 邮件连接上的站点，请标明此站点仅具有基于邮件的连接。

图 9.3 是假想的 Reskit 公司的网络拓扑。

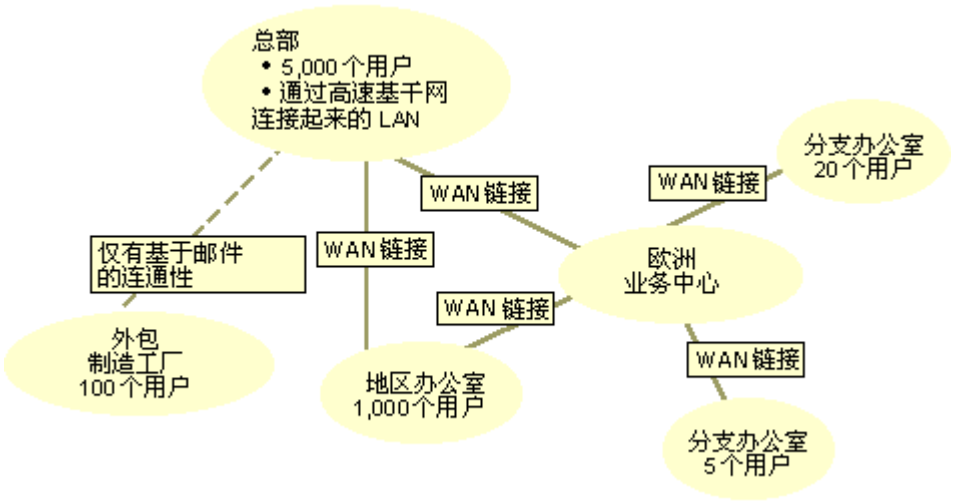


图 9.3 Reskit 公司网络拓扑

放置域控制器

Active Directory 的可用性取决于域控制器的可用性。域控制器必须是可用的，以便可以验证用户的身份。在该步骤中，您将确定放置域控制器的位置，以便在网络万一出问题时保持其可用性。

要放置域控制器，按以下步骤进行：

- 选择一个“主”站点，并将域控制器放入该站点中，方法是在拓扑布局图上标明它。

  可以任意选择主站点。例如，使用您的总部位置、用户数最多的站点或与网络的其余部分具有最好的总体连接的站点。主站点中的所有用户都用该域控制器来进行身份验证。现在可以忽略哪个域接受该域控制器服务，以及站点中必须有多少个此域的副本。

- 对于直接连接到主站点的每个站点，确定是否需要将域控制器放入这些站点中。

  或者不在这些站点中放入域控制器，而确定这些站点中的用户可否通过连回主站点中的域控制器的站点链接来进行身份验证。如果您能接受站点链接出故障时身份验证即告失败这一事实，则无需将域控制器放入这样的站点中。

  对于有客户计算机而无服务器的小型分支机构，不必采用域控制器。如果返回中央站点的链接出故障，该分支机构的用户还可以用缓存的凭据登录到他们的计算机上。没有必要进行进一步的身份验证，因为该分支机构中没有其它存放在服务器上的资源需要访问——所有资源都在中央站点上。

  在下列情况下，应将域控制器放入站点：

  - 站点中有大量用户，并且站点链接慢或已接近容量极限。在这种情况下，您不希望 Active Directory 客户通信占用链接容量。有关网络容量规划和由 Active Directory 客户产生的通信的详细信息，参见位于 http://windows.microsoft.com/windows2000/reskit/webresources 的“Web 资源”页上的 Microsoft Windows 2000 Server 链接。
  - 链接出现过不稳定的情况。不希望在链接不可用时身份验证失败。
  - 只能间断地使用链接。不希望身份验证在一天中的某段时间出故障或依赖于请求拨号链接。
  - 只能用 SMTP 邮件访问站点。如果只能通过 SMTP 邮件访问站点，用户必须有一个本地

域控制器来进行身份验证。

- 重复前面的过程以确定您需要将域控制器放入什么位置。

  将同样的过程应用到下一个相邻站点，直到访问了每个站点并确定是否有必要采用本地域控制器为止。

注意 域控制器包含对安全敏感的信息，例如用于域身份验证的用户密钥副本。这种信息的副本少一些，可以减少不经授权的访问的机会。必须用物理手段保护域控制器，以免非法访问。例如，建议将域控制器放在很少的人才能进入的锁好的房间内。入侵者可通过物理访问获取加密的密码副本，以将其用于脱机密码攻击。使用 Syskey 工具可以获得更安全的安全选择。有关 Syskey 的详细信息，参见 *Distributed Systems Guide* 中的 "Encrypting File System"。

当用户登录时，为身份验证请求提供服务的域控制器必须能够与全局编录服务器通讯。当决定将域控制器放入站点中时，也必须将该域控制器视为全局编录服务器。在您继续操作时，记住全局编录服务器产生的复制通信比普通域控制器产生的复制通信多。全局编录服务器既包含某个域的完整副本，也包含目录林中所有其它域的只读局部副本。

图 9.4 是 Reskit 公司的域控制器布置。

- 第一个域控制器放在总部所在地。
- 在欧洲运营中心放置了一个域控制器，因为跨洋 WAN 链接已接近容量极限。
- 在地区办公室也放置了一台域控制器，因为用户太多，WAN 无法传送身份验证通信。
- 分支机构不放置域控制器，因为分支机构没有本地服务器。
- 在制造工厂也放置了一台台域控制器，因为它只能通过 SMTP 邮件连接上。

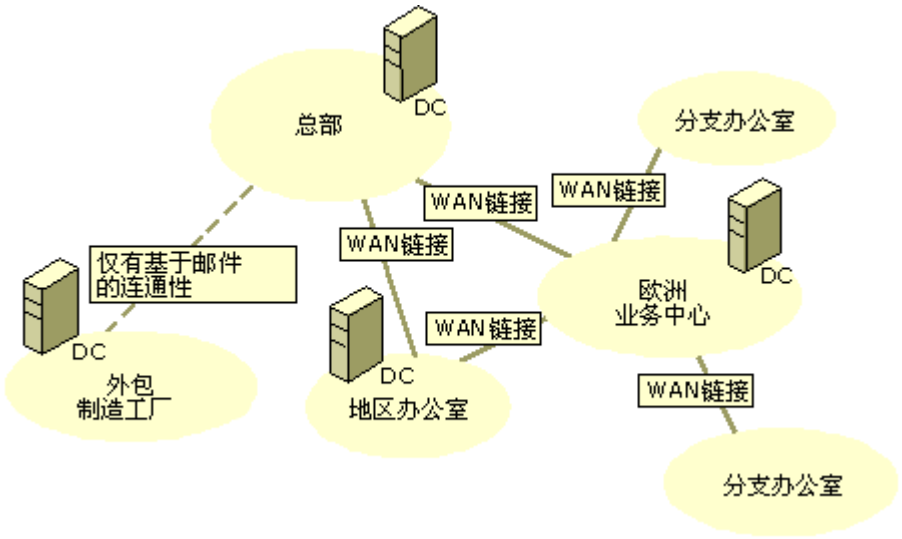


图 9.4 Reskit 公司域控制器布置

对目录林分区

现在您将为每个域控制器指派一个域，确定网络能否处理复制通信，而且如果必要，将目录林分区成更小的域。在做这些工作时，请记住分区的目的是要将目录对象的物理副本放到离需要这些对象的用户更近的地方。

例如，您需要将用户的用户帐户对象放在该用户所在站点内的域控制器上。

要对目录林进行分区，请为当前域规划中的每个域执行以下步骤：

- 对于包含域控制器的每个站点，请确定域是否与站点中的用户相关。如果合适，请将域的域控制器放入站点。
- 跟踪域中域控制器之间的复制将遵循的路径。假设每个域控制器将选择同一域的下一个最近的域控制器来作为复制伙伴，这里的“最近”由网络中最合算的路径来确定。
- 某个域中任何两个域之间的复制通信量问题，是一个域中对象更改频繁程度如何、有多少对象发生更改和添加与删除对象的频繁程度如何的因素。通过将域分成两个或更多个更小的域，您可以降低将通过某个特定链接传输的复制通信量。检查复制路径中的每个边缘，并确定是允许该复制通信还是拆分域。

在决定是否在站点之间复制某个域或是否将其分成两个或更多个更小的域时，请考虑这些因素。

- 如果复制路径中的站点链接不能容纳期望的复制通信，请考虑拆分域。

  站点链接的实际容量是链接速度、日常使用特征、可靠性和可用性的总体性能。在决定是否创建域时，请考虑以下有关链接的信息：

  - 在接近容量极限的情况下运行的链接可能无法适应复制。请记住，您可以对 Active Directory 复制进行日程安排，因此，如果链接在一天中有空闲时段，则可能会有足够的实际带宽来让复制进行下去。
  - 链接有可能仅在一天中的特定时段才可用，从而降低其实际带宽。可以将 Active Directory 复制安排到仅在链接可用时才发生，但实际带宽必须足够大，以容纳复制。

  有关网络容量规划和 Active Directory 复制通信的详细信息，参见位于 http://windows.microsoft.com/windows2000/reskit/webresources 的“Web 资源”页上的 Microsoft Windows 2000 Server 链接。

- 如果不希望复制通信与链接上的其它更重要的通信争夺带宽，可以考虑拆分域。

  中断或延迟与商务相关的通信可能比添加一个域的代价更高。

- 如果复制通信跨越按使用程度收费的链接，请考虑拆分域。

  如果某个链接是按使用程度收费的，尽量少使用它可以最大限度地降低成本。

- 为只能通过 SMTP 邮件连接的站点创建域。

  Active Directory 的基于邮件的复制只能在域之间进行。不可以将基于邮件的复制用于同一域的域控制器之间。

如果您确实决定将某个大型域分成几个更小的域，创建更小的域一个好策略是让它们基于地理边界或地缘政治边界。例如，创建映射为国家或洲的域。建议创建地理映射域，因为网络拓扑更趋于映射到地理位置，而地理关系比其它划分标准变化更少。

您可能仅仅为了优化网络上的复制通信而希望创建更多更小的域。请记住，优化与如下其它因素各有利弊：

- 复杂性

正如一开始讨论过的那样，每增加一个域都会耗费一定的常规管理开销。

- 查询通信与复制通信的对比

  域中的对象越少，该域中的用户希望访问其它域中的对象的可能性越大。如果其它域没有本地域控制器，查询会引起通信离开站点。

注意 单一的大型域模式最适合大量的漫游用户，因为在每个具有域控制器的站点上每个用户帐户都是可用的。在这种情况下，如果在用户的当前位置和主站位置之间出现网络故障，漫游用户也决不会丧失登录能力。

图 9.5 是 Reskit 公司的物理分区。域指派如下：

- 北美的用户 Noam 域被指派给主站点中的域控制器。
- 为进行管理而创建的 Avionics 域被指派给主站点中的域控制器，因为总部有 Avionics 用户。
- 一个新的域 Eu 被指派给欧洲运营中心的域控制器，因为跨洋 WAN 链接已接近容量极限。该链接无法处理北美和欧洲域组合的复制通信。
- Avionics 域还用于欧洲运营中心，因为欧洲有 Avionics 用户。
- 一个新的域 Seville 被指派给 Seville 的地区办公室中的域控制器，因为到欧洲运营中心的 WAN 链接在传送与商务相关的通信。
- 一个新的域 Mfg 被指派给制造工厂中的域控制器，因为只有 SMTP 邮件才能访问该工厂。

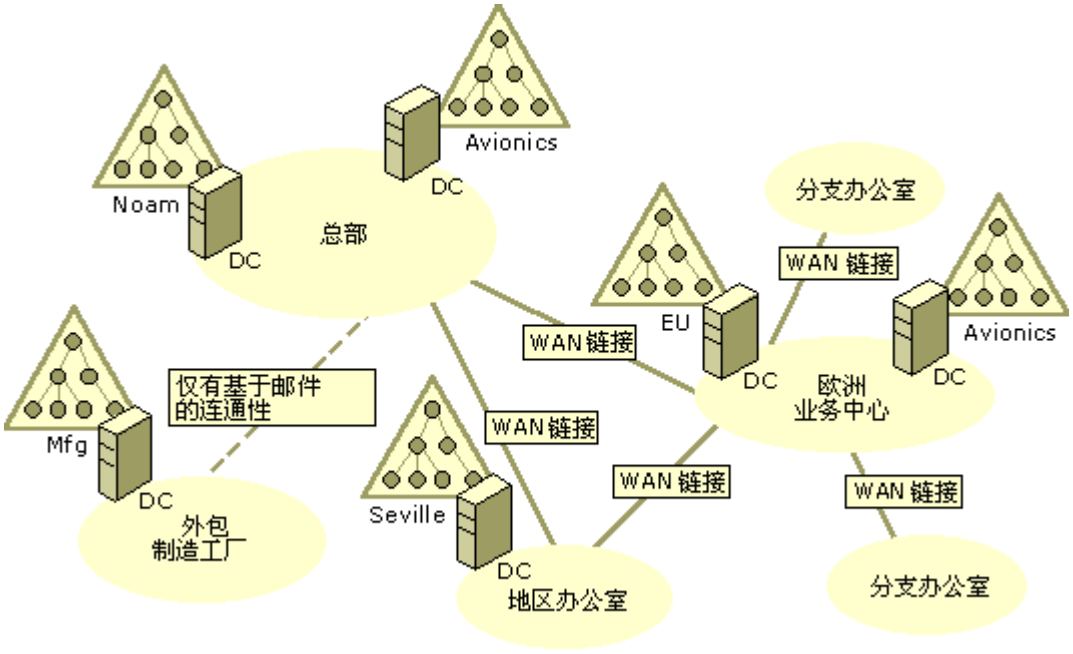


图 9.5 Reskit 公司域指派

增加域的成本增加

目录林中的每个域都会耗用一定的管理开销。在为是否在域规划中添加域而争论时，请将以下成本与您在本章前面确定下来的优点进行权衡。

更多的域管理员 由于域管理员完全控制域，所以必须对一个域的域管理员组的成员身份进行密切监控。目录林中每个添加的域都会产生这种管理开销。

更多的域控制器硬件 在 Windows 2000 中，一个域控制器只能主持一个域。您创建的每个域都需要至少一台计算机，并且在多数情况下，需要用两台计算机才能满足可靠性和可用性要求。因为所有 Windows 2000 域控制器都可以接受和产生更改，所以在对其进行物理监视时，必须比监视 Windows NT 4.0 备份域控制器 (BDC) 更加小心，其中后者是只读计算机。注意 Active Directory 域中的管理委派可以降低对资源域的要求。如果选择将域合并为更少的 Active Directory 域，某些目前必须主持两个域控制器（主用户域和本地资源域）的远程位置现在只需一个域控制器。

更多的信任链接 某个域中的域控制器如要对另一个域中的用户进行身份验证，它必须能够与第二个域中的域控制器取得联系。当两个域控制器之间的网络功能不正常时，这种通讯存在发生更多故障可能性。位于单一域中的用户和资源越多，单个域控制器就越没有必要依赖于与其它域控制器的通讯来维持服务。

必须在域之间移动安全主管的可能性更大 拥有的域越多，必须在两个域之间移动安全主管（例如用户和组）的可能性就越大。例如，业务重组或某个用户的工作更换就会产生在域之间移动用户的需要。对最终用户和管理员而言，在某个域中的部门之间移动安全主管是一种琐屑而透明操作。但是，在域之间移动安全主管涉及面更广，并且会影响最终用户。

有关在域之间移动安全主管的详细信息，参见本书中的“确定域迁移策略”。

组策略和访问控制不在域之间流动 应用于一个域中的组策略和访问控制不会自动流到其它域。如果有通过访问控制的策略和委派管理，而这些访问控制对许多域都是一致的，则必须将它们单独应用到每个域。

选择目录林根域

确定将要放入目录林中的域的数目后，您需要决定将哪个域作为目录林根域。目录林根域是您在某个目录林中创建的第一个域。企业管理员组和架构管理员组这两个目录林范围的组将驻留在此域中。

注意 如果目录林根域的所有域控制器在一次灾难性事故中丧失，而且一个或多个域控制器无法从备份恢复，您将永久丧失企业管理员组和架构管理员组。无法重新安装目录林的目录林根域。

如果目录林仅包含一个域，则该域为目录林根域。如果目录林包含两个或更多的域，考虑采用以下两种方法来选择目录林根域。

使用现有的域

从已有的域列表中，选择一个对您的单位运转起关键作用的域并将其作为目录林根域。因为丧失该域后果不堪设想，要求具有目录林根所要求的那种容错能力和可恢复性。

使用专用的域

创建另外一个、专用域来单独充当目录林根会需要承担额外的域的所有成本，但它也可能给本单位带来一定的利益，例如：

- 目录林根域中的域管理员将能够操纵企业管理员和架构管理员组的成员身份。您可能有一些管理员，他们需要域管理员特权用于其部分职责，但您不希望他们能操纵目录林范围的管理员组。通过单独创建一个域，您就不必将这些管理员放入目录林根域的域管理员组。
- 由于该域较小，所以可以在网络上的任何位置复制它，以防止集中在某个地理位置发生灾难。
- 由于该域的唯一作用是充当目录林根，所以它没有过时的风险。当您从一个规划好的域列表中选择

域来作为目录林根时，始终有特定的域过时的可能，其原因可能是因本单位发生变化。但是，您将永远无法淘汰一个这样的域，因为它必须起目录林根的作用。

指派 DNS 名称以创建域层次结构

Active Directory 域是用 DNS 名来命名的。由于 DNS 是 Internet 上最流行的命名系统，所以全球都能识别 DNS 名，而且它还有著名的注册机构。请求登录网络的 Active Directory 客户查询 DNS 来定位域控制器。

在 Windows NT 4.0 中，域定位器是基于网络基本输入/输出系统 (NetBIOS) 命名系统 (NBNS) 的，而且域是用 NetBIOS 名来识别的。基于服务器的 NBNS 组件称为 Windows Internet Name Service (WINS) 服务器。NetBIOS 是仅有一个部分的简单名称，并且无法对 NetBIOS 名称空间进行分区。与此相反，DNS 名是层次化的结构，而且可以沿着层次结构线对 DNS 名称空间进行分区。结果，DNS 比 NBNS 可扩展性更强，而且可以容纳分布在大型网络上的更大的数据库。Internet 邮件支持 DNS 的方式类似于 Active Directory，是将作为定位机制的 DNS 如何升级到像 Internet 这样的超大型网络的好例子。

注意 为实现与运行早期 Windows 版本的计算机的互操作，Active Directory 域具有 NetBIOS 名，并且在必要时，Active Directory 域控制器在 NBNS 中注册并查询 NBNS。这允许运行早期版本的 Windows 的客户定位 Active Directory 域控制器，并允许 Active Directory 域控制器和 Windows NT 3.51 与 Windows NT 4.0 域控制器相互进行定位。

将域分进目录树

目录树是具有连贯名称的一个或多个 Windows 2000 域的集合。图 9.6 是具有连贯名称空间的单一目录树的图解。由于 reskit.com 没有父域，所以它被视为目录树根域。reskit.com 的子域为 eu.reskit.com 和 noam.reskit.com。reskit.com 的孙子域为 mfg.noam.reskit.com。这些域名是连贯的，因为每个名称与域层次结构中它上面的域的名称仅相差一个标签。

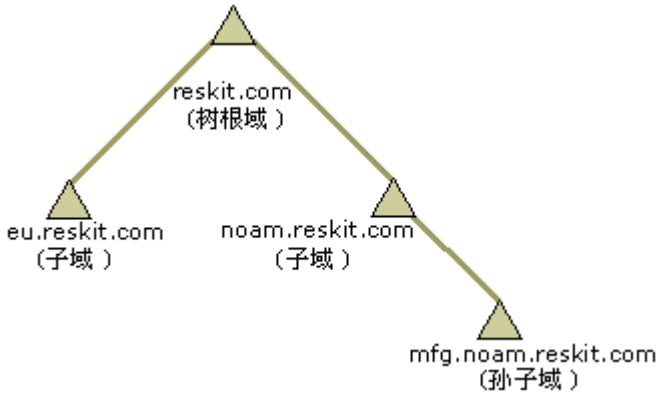


图 9.6 具有四个域的单一目录树

一个目录林可以有多个目录树。在一个多目录树目录林中，目录树根域名称是不连贯的，如图 9.7 所示。如果本单位中的某个部门拥有自己的已注册 DNS 名称并运行自己的 DNS 服务器，您可以在目录林中拥有多个目录树。

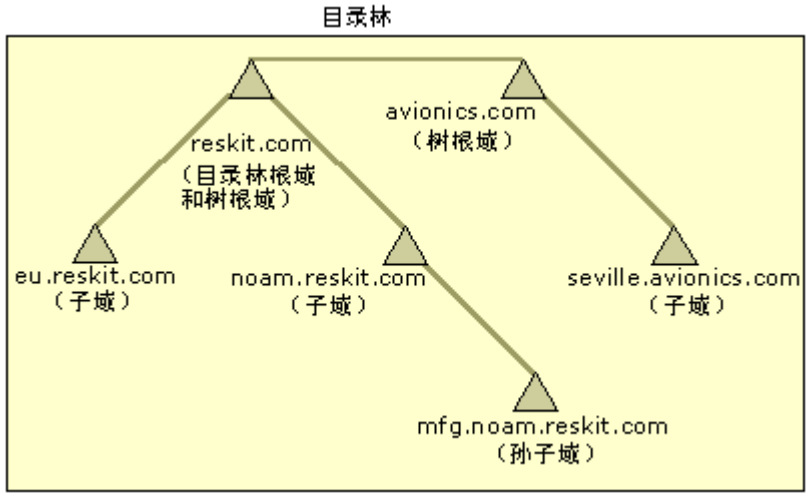


图 9.7 具有多个目录树的目录林

目录林中的域层次结构确定连接各个域的可传递信任链接。每个域同其父域或子域都有一个直接信任链接。如果目录林中有多个目录树，则从信任角度看，目录林根域在信任目录树的顶端，所有其它目录树根是子域。图 9.8 是两个目录树之间的可传递信任关系的图解。

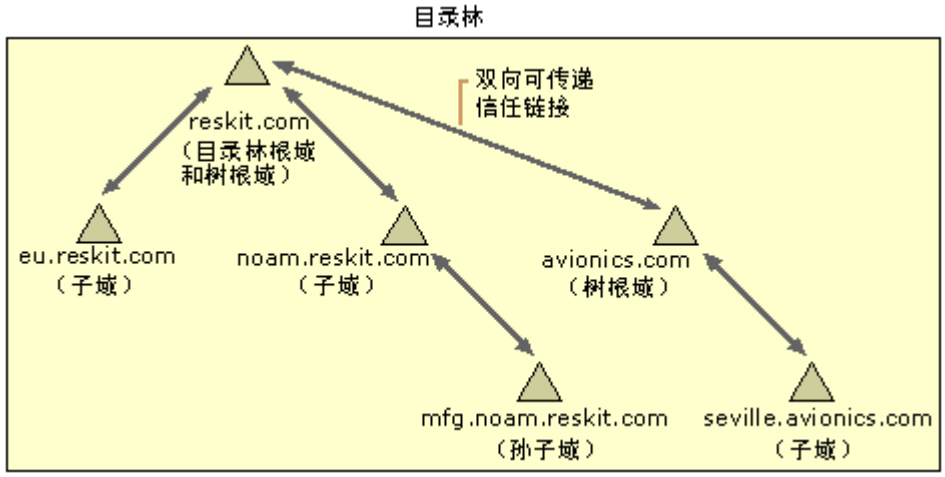


图 9.8 目录树之间的可传递信任关系

父子关系仅仅是一种命名和信任关系。父域中的管理员不会自动成为子域中的管理员。父域中的策略设置不能自动应用于子域。

域命名建议

要在目录林中创建域层次结构，将 DNS 名指派给第一个域，然后对以后的每个域，确定它是某个现有域的子域还是一个新的目录树根。在这一评估基础上，相应地指派名称。以下是命名域的一些建议：

使用相对于已注册 Internet DNS 名的名称。

已在 Internet 上注册的名称是全球唯一的。如果有一个或多个已注册 Internet 名称，在 Active Directory 域

名称中将这些名称用作后缀。

使用 Internet 标准字符。

Request for Comments (RFC) 1123 定义了用于 DNS 主机名称的 Internet 标准字符，它们为 A–Z、a–z、0–9 和连字符 (–)。仅使用 Internet 标准字符可以确保 Active Directory 适应基于标准的软件。为支持将基于早期 Windows 版本的域升级到具有非标准名称的 Windows 2000 域，Microsoft 客户程序和 Windows 2000 DNS 服务支持名称中的任何 Unicode 字符。

一定不要将同一名称使用两次。

一定不要将同一名称指派给两个不同的域，即使这些域位于具有不同 DNS 名称空间的未连接上的网络上。例如，如果 Reskit 公司决定将 Intranet 上的某个域命名为 reskit.com，该公司不应当同时在 Internet 上创建一个名为 reskit.com 的域。如果 reskit.com 客户同时连接到 Intranet 和 Internet，该客户将选择在定位搜索过程最先响应的域。对客户来说，这一选择是随机的，无法保证客户选择到“对口”的域。举一个这种配置的例子，已建立通过 Internet 连到 Intranet 的虚拟专用网络连接的客户。

使用有区别的名称。

某些代理客户软件（例如 Microsoft® Internet Explorer 中的内置代理客户软件和 Winsock Proxy 客户软件）使用主机的名称来确定主机是否在 Internet 上。这种类型的软件多数至少要提供一种方法，此方法排除带特定后缀的名称作为本地名称，而不假定这些名称是在 Internet 上。

如果 Reskit 公司希望将其 Intranet 上的 Active Directory 域命名为 reskit.com，必须在其代理客户软件的不重名列表上输入 reskit.com。这可以防止 Reskit Intranet 上的客户在 Internet 上看到一个名为 www.reskit.com 的主机，除非该公司在 Intranet 上有一个同样的站点。

要避免这种问题，Reskit 公司可以使用一个未出现在 Internet 上的注册名，例如 reskit-int01.com；或制定公司策略，声明以 reskit.com 特定后缀结束的名称，例如 corp.reskit.com，不得出现在 Internet 上。在这两种情况下，配置代理客户不重名列表以确定哪些名称用于 Intranet 上，哪些名称用于 Internet 上是很容易的。

从专用 Intranet 访问 Internet 有许多不同技巧。在使用任何名称之前，确保在您的专用 Internet 访问策略内，您 Intranet 上的客户可以正确地解析它。

尽可能少使用目录树。

最大限度地减少目录林中的目录树有多种优点。下列优点可应用于您的环境中：

- 在取得特定 DNS 名的控制权后，您就拥有了从属于该名称的所有名称。目录树越少，本单位中必须拥有的 DNS 名称数就越少。
- 需要在代理客户排除后缀列表中输入的名称就更少。
- 不是 Microsoft 客户的 LDAP 客户计算机在搜索目录时可以不使用全局编录。相反，为了执行目录范围的搜索，这些客户将使用深层搜索。深层搜索覆盖特定子目录树中的所有对象。目录林中的目录树越少，您为了覆盖整个目录林而必须执行的深层搜索就越少。

让 DNS 名的第一部分与 NetBIOS 名相同。

将完全不相关的 DNS 名和 NetBIOS 名指派给某个域是可能的。例如，域的 DNS 名可以是 sales.reskit.com，但 NetBIOS 名可是“Marketing”。记住 Windows 2000 之前的计算机和不支持 Active Directory 的软件将显示和接受 NetBIOS 名；而 Windows 2000 计算机和支持 Active Directory 的软件将显示和接受 DNS 名。这有可能给最终用户和管理员带来混乱。

如果存在下列情况，您只能使用不匹配的 NetBIOS 和 DNS 名：

- 希望迁移到网络上的新命名约定。
- 您正在升级的 NetBIOS 名包含非标准字符，而又希望 DNS 名全都使用标准字符。

从世界范围审查名称。

在一种语言中具有亲切感和有益含义的名称有时在另一种语言中则是贬义和冒犯别人的。DNS 是全局名称空间，确保从全球角度审查本单位内的名称。

注意 如果网络上运行了多个本地化 Windows 版本，则所有的计算机，包括运行 Windows 2000 Professional 和 Windows 2000 Server 所有版本的计算机，在其 DNS 和 NetBIOS 名称中都必须只使用标准 Internet 字符。如果使用上述字符以外的字符，则只有具有相同区域设置的计算机才能相互通讯。

使用简短易记的名称。

选择名称时，长度不应当是一个重要的决定因素。用户通常与全局编录交互，并不关心域名。一般只有管理员才会接触域名。管理工具始终会提供一个域列表来供您选择，需要管理员键入完整名称的情况属于例外，这不是常见的。一般来说，如果您能记住某个名称的所有部分，则说明它不太长。

域名和计算机名

默认情况下，加入某个域的 Windows 2000 计算机会给自己指派一个 DNS 名，该名称由这台计算机的主机名和它所加入的域的 DNS 名组成。例如，在图 Figure 9.9 中，如果 Server 1 的计算机帐户位于 eu.reskit.com 中，则这台计算机会默认地将自己命名为 server1.eu.reskit.com。但是，用任意 DNS 后缀来代替 Active Directory 域名也是可能的。由于这个原因，没有必要这样命名 Active Directory 域，以使其适合已部署到本单位中的 DNS 结构。Active Directory 域可以使用任何名称，并且计算机可以保留其现有名称。

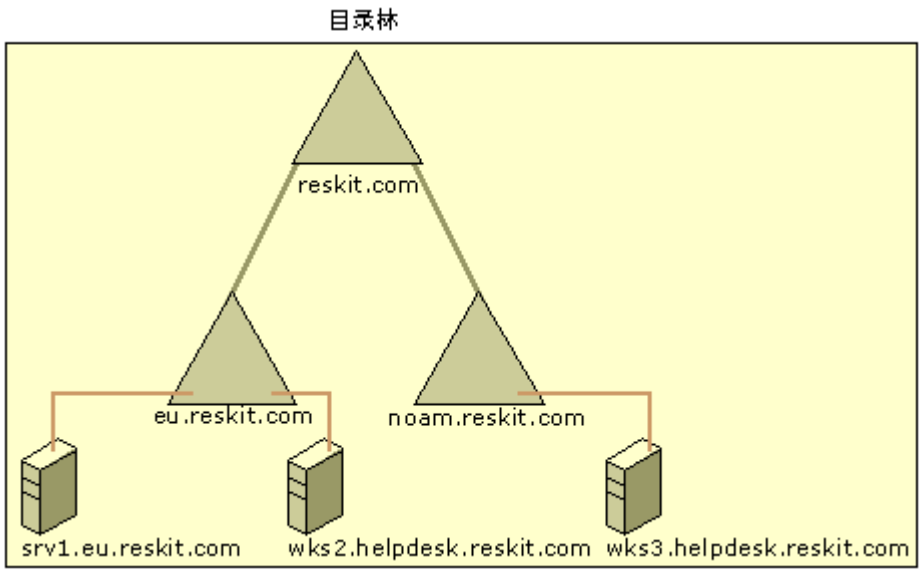


图 9.9 具有默认名称和非默认名称的成员计算机

有关计算机命名的详细信息，参见 *TCP/IP Core Networking Guide* 中的“Windows 2000 DNS”。

规划 DNS 服务器部署

要规划 DNS 服务器部署以支持 Active Directory 域，必须确定将要负责域名的 DNS 服务器，并确保它们满足域控制器定位器系统的要求。

DNS 中的颁发机构和委派

域名系统是一个分层的分布式数据库。数据库本身是由资源记录组成，资源记录主要包括 DNS 名称、记录类型以及与该记录类型相关的数值。例如，DNS 数据库中最普通的记录是地址 (A) 记录，地址记录中的名称是计算机名，记录中的数据是该计算机的 TCP/IP 地址。

和 Active Directory 一样，DNS 数据库分成多个分区，这样即使在很大的网络中数据库也可有效地伸缩。DNS 数据库的分区称为“区域”。一个区域包含一组连续的 DNS 名称的记录。加载了区域的 DNS 服务器负责该区域中的名称。

区域从一个指定名称开始，在委派点结束。委派点指出一个区域结束和另一个区域开始的位置。例如，在 Internet 中有一个负责称为“com”的区域的注册颁发机构。在这个区域中有成千上万个到其他区域的委派点，例如 reskit.com。委派点中的数据指出哪些服务器负责委派的区域。图 9.10 显示了 DNS 服务器、区域和委派之间的关系。

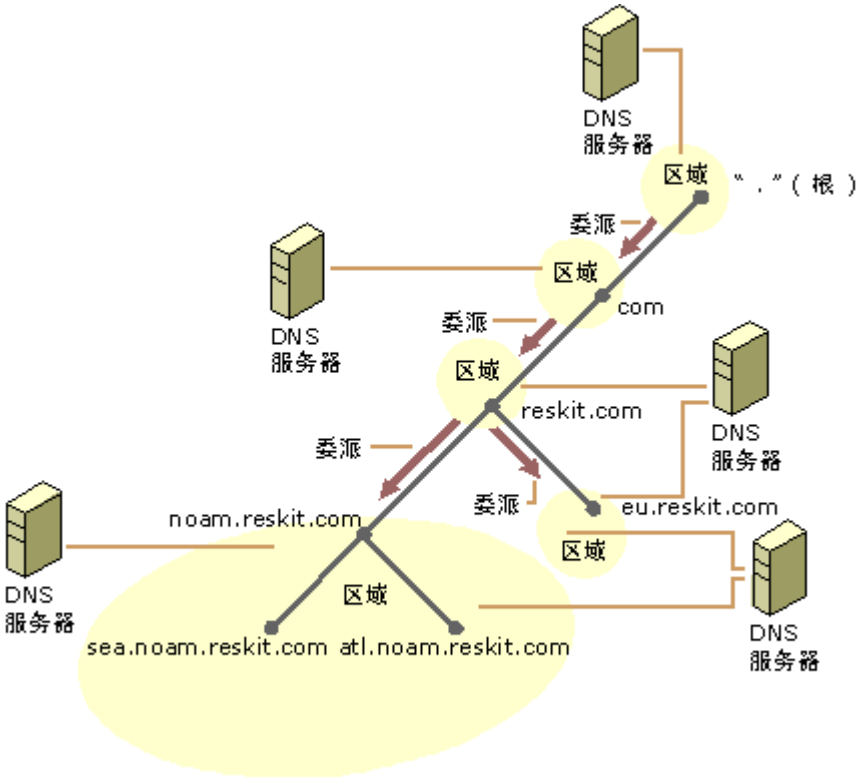


图 9.10 DNS 中的服务器、区域和委派

域控制器定位器系统

域控制器在 DNS 中注册一组记录。这些记录被统一称为定位器记录。当客户需要一个域的特别服务时，它为一个特定名称和类型的记录发送一个查询到最近的 DNS 服务器。应答是一个可以满足该请求的的域控制

器的列表。

每个域的定位器记录的名称以 *<DNS-domain-name>* 和 *<DNS-forest-name>* 结束。负责每个 *<DNS-domain-name>* 的 DNS 服务器将负责定位器记录。

备注 Windows 2000 并不要求配置反向搜索区域。反向搜索区域可能对于其他应用程序是必需的，或者是为了实现管理上的便利。

DNS 服务器要求

如果还没有 DNS 服务器在网络上运行，建议您部署 Windows 2000 Server 提供的 DNS 服务。如果已有 DNS 服务器，那么负责定位器记录的服务器必须满足下列要求以支持 Active Directory：

- 必须支持服务定位资源记录。

  负责定位器记录的 DNS 服务器必须支持“服务位置 (SRV)”资源记录类型。有关 SRV 记录的详细信息，请参见 *TCP/IP Core Networking Guide* 中的“Introduction to DNS”。

- 应该支持 DNS 动态更新协议。

  负责定位器记录并作为这些区域的主服务器的 DNS 服务器应该支持在 RFC 2136 中定义的 DNS 动态更新协议。

Windows 2000 Server 提供的 DNS 服务同时满足这些要求，并且还提供两个重要的附加功能：

- Active Directory 集成

  使用这个功能，Windows 2000 DNS 服务把区域数据存储在目录中。这使得 DNS 复制创建多个主机，并允许任意 DNS 服务器接收关于集成了目录服务的区域更新报告。使用 Active Directory 集成也减少了对维护一个单独的 DNS 区域传送复制拓扑的要求。

- 安全动态更新

  安全动态更新与 Windows 安全集成。它使得一个管理员可以精确地控制哪些计算机可以更新哪些名称，并防止未经授权的计算机从 DNS 获得现有的名称。

网络上其余的不负责定位器记录的 DNS 服务器不需要满足这些要求。不负责的服务器通常可以应答 SRV 记录查询，即使它们并不明确支持该记录类型。

定位授权服务器

对于所选择的每个 DNS 名称，咨询您的 DNS 管理组并查明 DNS 服务器是否支持所列出的要求。如果找到一个不支持的服务器，可以采取三种基本的操作方法：

将服务器升级到一个支持这些要求的版本。

如果授权服务器正在运行 Windows NT 4.0 DNS 服务，只需将这些服务器升级到 Windows 2000。对于其他的 DNS 服务器，参考供应商的文档确定哪些版本支持 Active Directory 所要求的功能。

如果授权 DNS 服务器并不在您的控制之下，也不能说服这些服务器的所有者进行升级，那么可以选择另一种方法。

迁移区域到 Windows 2000 DNS。

可以将区域从授权服务器迁移到 Windows 2000 DNS，而无需将这些服务器升级到支持 Active Directory 要求的版本。迁移区域到 Windows 2000 DNS 是一个很简单的过程。引入一个或多个 Windows 2000 DNS 服务器作为区域的辅助服务器。对服务器的性能和可管理性感到满意之后，将一个服务器的区域转换为主拷贝，并在必要时重新安排 DNS 区域转换拓扑。

委派名称给一个满足要求的 DNS 服务器。

如果升级和迁移授权服务器都不是合适的选择，可以通过委派域名到 Windows 2000 DNS 服务器来更改授权服务器。如何具体实施取决于域名与现有的区域结构的关系。

- 如果域名与区域的根的名称不同，那么可以直接委派域名到 Windows 2000 DNS 服务器。例如，如果域的名称是 noam.reskit.com 而包含这个名称的区域是 reskit.com，委派 noam.reskit.com 到 Windows 2000 DNS 服务器。
- 如果域名与区域的根的名称相同，那么不能直接委派域名到 Windows 2000 DNS 服务器。
- 委派定位器记录使用的每个子域到一个 Windows 2000 DNS 服务器。
- 这些子域是：_msdcs.<*DNS-domain-name*>、_sites.<*DNS-domain-name*>、_tcp.<*DNS-domain-name*> 和 _udp.<*DNS-domain-name*>。如果这样，必须手动地注册 <*DNS-domain-name*> 地址 (A) 记录。
- 有关这个主题的详细信息，请参见 *TCP/IP Core Networking Guide* 中的“Windows 2000 DNS”。

用快捷信任关系优化身份验证

当用户要求访问网络资源时，用户域的域控制器必须与资源域的域控制器通信。如果两个域不是父子关系，用户的域控制器也必须与用户域和资源域之间的信任目录树中每个域的域控制器通信。根据域控制器在每个域中的网络位置，两域之间额外的身份验证跃点会增加失败的可能性，或增加身份验证通信必须通过慢速链接的可能性。要减少这些交互所必需的通信的数量，可以使用“快捷信任”关系连接任意两个域。

例如，如果在目录林中有多个目录树，可能要在一个完整的信任网格中连接目录树根组。记住在默认安排中，所有的目录树根从信任的观点来看都被认为是目录林根的子目录树根。这意味着任何位于不同目录树中的两个域的身份验证通信都必须通过目录林根。创建一个完整的信任网格使得任意两个目录树根域可以相互直接通信。

图 9.11 显示了在四个目录树根域之间创建的一个完整的信任网格。

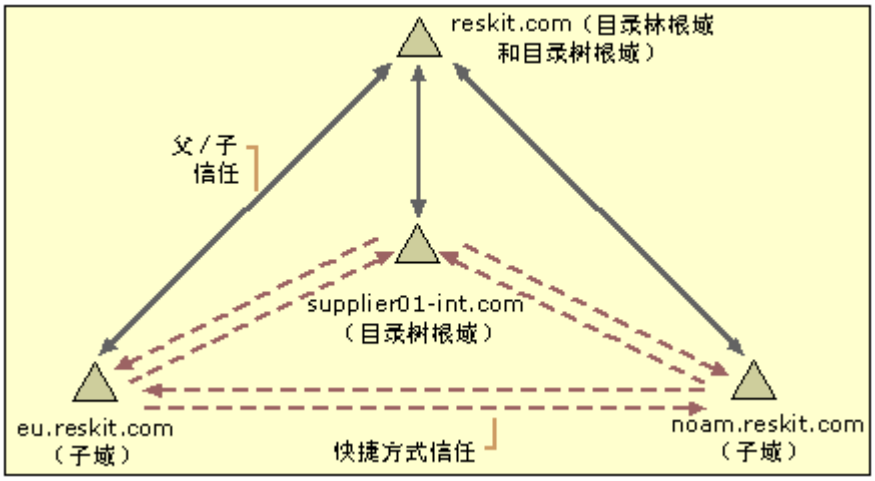


图 9.11 四个域之间的完整的信任网格

在部署后改变域规划

创建了域层次结构之后就不太容易对它们进行更改。由于这个原因，最好不要创建基于临时或短期存在的组织结构的域。例如，创建了一个映射到单位特定业务部门的域，当公司重组时，该业务部门可能会被分割、解散或与其他部门合并，这时您就需做些工作了。

但是，在有些情况下基于单位进行分区是适当的。地理政治学边界是一个进行分区的相对稳定的模板，但只有当单位不经常超出边界移动时。考虑一支部队的域规划，该部队在几个基地有不同的分部。可能分部在不同的基地之间移动是很普遍的。如果目录林是根据地理位置进行分区的，当一个分部在基地之间移动时，管理员需要在域之间移动大量的用户帐户。如果目录林是根据分部进行分区的，管理员只需在基地之间移动域控制器。在这种情况下，基于单位进行分区将比地理分区更合适。

添加新域和删除现有域

可以很容易地把新域添加到目录林中，但是不能在目录林之间移动现有的 Windows 2000 Active Directory 域。

◆	**关键的决定点** 建立了目录树根域之后，不能使用一个更高级名称添加域到目录林。不能创建现有域的父域，只能创建子域。例如，如果目录树中的第一个域称为 eu.reskit.com，就不能以后再添加一个称为 reskit.com 的父域。

把域中所有的域控制器降级到成员服务器或单机角色，将从目录林中删除域并删除保存在域中的所有信息。只有在域没有子域时才能将它从目录林中删除。

合并和拆分域

Windows 2000 不提供在单一操作中将一个域拆分为两个域或将两个域合并为一个域的能力。

◆	**关键的决定点** 设计好域规划以争取在单位发展时只需做最少的分区更改是很重要的。

可能通过添加一个空域到目录林然后将对象从其他域移到该域来拆分一个域。同样，也可能通过将源域中的

所有对象移到目标域来实现域的合并。正如前面所提到的，在域之间移动“ 安全主管 ”可以影响最终用户。有关在域之间移动对象的详细信息，请参见本书的“ 确定域迁移策略 ”。

重命名域

Windows 2000 不提供原位重命名域的能力。因为域的名称也代表它在目录树层次结构中的位置，同时域也不能在目录林中移动。

关键的决定点 当为域选择名称时，选择那些随着单位的发展将一直有意义的名称。

对原位重命名的变通方法是使用所期望的新名称在目录林中创建一个新的域，然后将所有的对象从原来的域移到新的域。

制定部门规划

部门 (OU) 是一个用来在域中创建结构的容器。在域中创建结构时，考虑 OU 的下列特性是很重要的。

OU 可以是嵌套的。一个 OU 可以包含子 OU，使得可以在域中创建一个分层的目录树结构。

OU 可以用来委派管理和控制对目录对象的访问。当综合使用 OU 嵌套和访问控制列表时，可以用一种非常细化的方式委派目录中对象的管理。例如，可以赋予帮助中心技术人员权限，为一组指定的用户重新设置密码，但无权创建用户或修改用户对象的任何其他属性。

OU 不是安全主管。不能使 OU 成为安全组的成员，也不能因为用户驻留在特定的 OU 中而授予他们访问资源的权限。因为 OU 用于管理的委派，所以用户对象的父 OU 指出谁管理用户对象，但是它并不指出用户可以访问的资源。

组策略可以与一个 OU 相关联。组策略使您可以定义用户和计算机的桌面配置。可以将组策略与站点、域和 OU 相关联。在 OU 基础上定义组策略使您可以在同一域中使用不同策略。有关组策略的详细信息，请参见本书中的“ 应用更改和配置管理 ”以及“ 定义客户管理和配置标准 ”。

用户不会在 OU 结构中浏览。没有必要设计一个吸引最终用户的 OU 结构。尽管用户有可能浏览一个域的 OU 结构，但对于用户查找资源来说，这并不是一个最有效的方法。在目录中查找资源的最有效的方法是查询全局编录。

OU 结构和业务结构

“ 部门结构 ”这个词可能首先会让您想到创建一个反映业务单位和它的不同分支、部门和项目的结构。可以创建这样一个结构，但可能发现它难以管理并且费用高昂。OU 用于委派管理，所以创建的结构很可能是管理模型的映射。单位的管理模型可能并没有准确地映射业务单位。

例如，考虑图 9.12 中显示的基于业务的结构。.已经为家用电子（电子 OU）、医疗系统（医药 OU）和汽车（汽车 OU）分部创建 OU，其中汽车部门的用户在汽车 OU 中，以此类推。

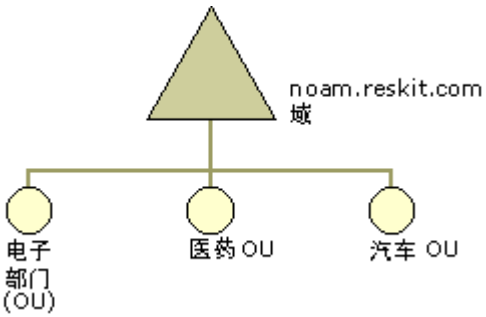


图 9.12 根据业务结构制定的 OU 结构

假设本例中的公司使用一种集中管理的模式。一组管理员管理公司的所有用户而不区分业务部门。在公司的日常运作中，可能会出现很多情况。如果一个人在家用电子分部和汽车分部之间调动，管理员必须将此人的用户帐户从电子 OU 移到汽车 OU。如果人员的调动很多，对于管理组来说，这将累积成为一个相当大的工作量。但实际上完成了什么呢？

对于同一公司，可以考虑一个只包含一个 OU 的 OU 结构，该 OU 包含了所有用户帐户。如果用户在分部之间调动，移动对象不需要管理员的额外工作。无论何时创建结构，确保它服务于一个明确的目的。不合理的结构将导致不必要的工作量。

可能需要在 OU 结构中映射业务结构，使得生成一个基于业务单位的用户列表比较容易。使用 OU 只是达到这个目的的一个方法。业务结构可能更真实地反映资源访问授予给用户的方式。例如，做某个项目的用户可能会被允许访问一组特定的文件服务器，或者某分部的用户可能会被允许访问一个特定的 Web 站点。因为资源访问使用安全组授权，所以可能会发现业务组织结构在安全组结构中得到了更好的体现，而非在 OU 中。

OU 规划过程

为域创建一个 OU 结构的步骤如下：

- 创建 OU 以委派管理。
- 创建 OU 以隐藏对象。
- 为组策略创建 OU。
- 理解部署之后更改 OU 结构的影响。

遵循上面顺序中的步骤是很重要的。您将发现一个完全为管理委派而设计的 OU 结构与一个完全为组策略而设计的 OU 结构不同。因为有多种方法应用组策略，但只有一种方法委派管理，所以应该首先为管理委派创建 OU。

OU 结构将很快变得相当复杂。每次添加一个 OU 到规划中时,要记下创建的具体原因。这有助于确保每个 OU 有一个目的，并将帮助阅读规划的人理解结构所基于的理由。

当为每个域创建 OU 规划时，咨询管理单位中的下列组：

- 负责用户帐户、安全组和计算机帐户的现任域管理员。
- 现有资源域的所有者和管理员。

创建 OU 以委派管理

在 Windows 2000 之前的 Windows NT 版本中，域的管理委派仅限于使用内建的本地组，例如帐户管理组。这些组有预先定义的功能，在某些情况下这些功能并不符合特殊情况的要求。结果，在某些情况下，单位中的管理员需要高级的管理访问（例如域管理员）权限。

在 Windows 2000 中，管理委派功能更强并更具灵活性。这种灵活性是通过部门、每个属性访问控制和访问控制继承的组合来实现的。管理可以任意委派，其方法是通过授予一组用户创建特定类别的对象、或修改特定类别的对象的特定属性的能力来实现。

例如，可以授权人力资源部门在特定的 OU 中创建用户对象，而不在其他地方。可以授权帮助中心技术人员重新设置该 OU 中的用户的密码，但不能创建用户。可以授权其他的目录管理员修改用户对象的通讯簿属性，但不允许创建用户或重新设置密码。

在单位中委派管理有一些好处。委派特定的权限使您可以将必须有高级访问权限的用户的数量降到最少。权限受到限制的管理员所发生的事故或错误所产生的影响只限于他们负责的范围。以前，在单位中除了 IT 之外的组可能必须将更改请求提交到高级管理员，高级管理员代表他们进行更改。通过管理委派，可以将责任分散到单位中的各个组，这样可以节省将请求发送到高级管理组的开销。

修改访问控制列表

要委派管理，授予一个组对 OU 的特定权限。要做到这一点，需要修改 OU 的访问控制列表 (ACL)。一个对象的 ACL 中的访问控制项 (ACE) 决定谁可以访问该对象以及可以进行哪种类型的访问。当在目录中创建一个对象时，默认的 ACL 将应用于对象。默认的 ACL 在对象类别的架构定义中介绍。

ACE 可以被容器对象的子对象继承。如果子对象也是容器，ACE 也将应用到这些容器的子对象。通过继承，可以将委派权利应用到 OU 的整个子目录树而不是单个 OU。也可以通过阻止一个对象的 ACE 继承来防止父容器的 ACE 应用到该对象或它的任何子对象。继承的 ACE 只在域中应用而不应用于子域。

要委派对 OU 子目录树中的一组对象的控制，可以编辑 OU 的 ACL。要做到这一点，最简单的方法是使用用于 Active Directory 用户和组的 Microsoft 管理控制 (MMC) 管理单元中的控制委派向导。要查看一个对象的 ACL 或执行 ACL 的高级编辑，使用对象的属性页的“安全”选项卡。

经常参考 ACL 中的组而不是单独的用户。管理一个组的成员身份要比管理一个 OU 中的 ACL 简单。当用户改变角色，发现和改变他们的组成员身份要比检查每个 OU 的 ACL 容易得多。如果可能，委派到本地组而不是全局组或通用组。不同于全局组，本地组可以有来自任何受信域的成员，使他们更适合授予资源权限。不同于通用组，本地组成员身份并不复制到全局编录，使得本地组资源较少。

确定创建何种 OU

创建的 OU 结构将完全取决于管理是如何在单位中委派的。委派管理的三种方法是：

- 按物理位置。例如，欧洲的对象可以通过一组自治的管理员进行管理。
- 按业务单位。例如，属于 Avionics 分部的对象可以通过一组自治的管理员进行管理。
- 按角色或任务。这个分部依照对象被管理的类型。例如，一组管理员可能只负责计算机帐户对象。

这三个方法经常结合使用。例如，如图 9.13 所示，可有一个管理组负责汽车业务单位的位于亚特兰大的计算机帐户对象。

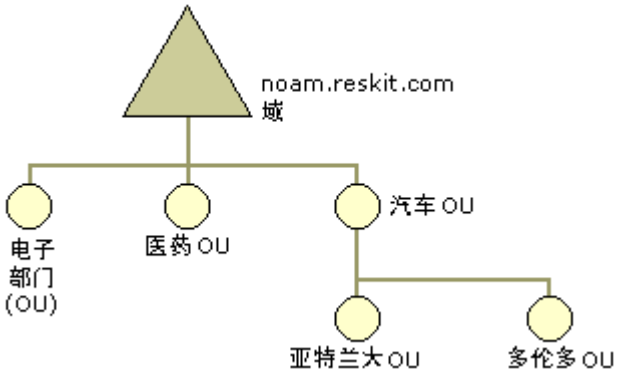


图 9.13 双重委派

亚特兰大 OU 是否是汽车 OU 子部门取决于汽车的管理员是否委派权限给亚特兰大的管理员，或者反之亦然。也可能亚特兰大的管理员相对于汽车的管理员是完全自治的，因此，这两个 OU 是平等的。

注意 一些单位在地理上将管理组分散以支持 24 小时运行。所有管理组的正常工作时间合在一起能满足该单位 24 小时运行的需要。在这种情况下，每个管理组的作用域并不针对特定位置，因为管理员必须能够为世界各地的用户提供支持。尽管在这种情况下管理员分布于许多位置，但它仍不是基于位置的委派的情况。

委派步骤

从域中的默认结构开始，按下列主要步骤创建 OU 结构：

- 通过委派完全控制创建 OU 的顶层。
- 创建 OU 的下层来委派每个对象类别控制。

委派完全控制

开始，只有域管理员拥有对所有对象的完全控制。理论上说，域管理员应该只负责：

- 创建初始的 OU 结构。
- 修改错误。

  域管理员不仅拥有默认的完全控制，他们也具有取得域中任何对象的所有权的权限。使用这个权限，域管理员可以获得对域中任何对象的完全控制，而不论该对象的权限设置如何。

- 创建附加的域控制器。

  只有域管理员组的成员可以为一个域创建附加的域控制器。

因为域管理员可以具有有限的和特定的责任，可以使组的成员身份小而可控制。

如果需要允许单位中的部门确定他们自己的 OU 结构和他们自己的管理模式，使用下列步骤：

- 为每个部门创建一个 OU。
- 为每个部门创建一个本地组，代表该部门的最高级管理员。
- 指派相应组完全控制它的 OU。

- 如果允许该部门设置它的成员身份，将该部门的管理员组放置到 OU中。如果不允许该部门设置它自己的管理员成员身份，将该组放置在 OU 之外。

委派完全控制示例

Reskit 公司的汽车部门是由两个公司合并而成，其中汽车部门保留了一个完全自治的 IT 组。在这种情况下，汽车部门从域的根下获得它自己的 OU。因为允许定义他们的管理员组的成员身份，该组放置在汽车 OU 中。如果汽车部门在亚特兰大和多伦多有完全独立的业务，汽车的管理员可能再次创建 OU 并委派完全控制。如图 9.14 所示，汽车的管理员保留了设置亚特兰大和多伦多管理员组的成员身份的能力。

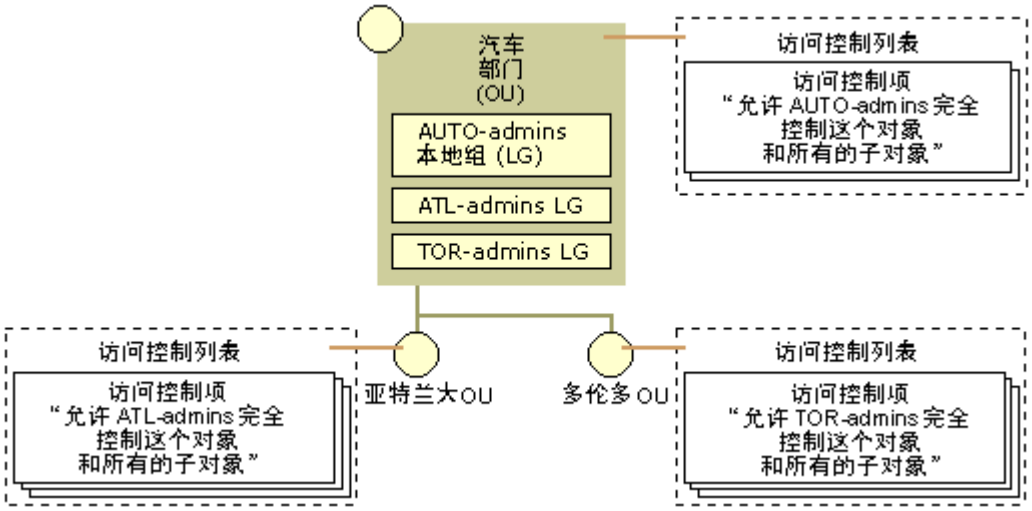


图 9.14 委派完全控制

如果在单位中没有需要完全控制的部门，域管理员将决定 OU 结构的其他部分。

委派每个对象类别控制

具有完全控制的组可以决定是否需要附加的 OU 以委派限制更严格的控制。一个简单的方法是考虑将在目录中创建的每个对象类别，并确定该对象类别的管理是否在单位中进一步委派。尽管架构定义许多种类的对象类别，只需考虑管理员将在 Active Directory 中创建的对象类别。至少应该考虑：

- 用户帐户对象
- 计算机帐户对象
- 组对象
- 部门对象

在检查每个对象类别的同时，单独考虑：

- 应该给哪些组授予对一个特定类别的对象的完全控制？具有完全控制的组可以创建和删除指定类别的对象并修改指定类别的对象的任何属性。
- 应该允许哪些组创建特定类别的对象？默认情况下，用户对他们创建的对象具有完全控制。
- 应该只允许哪些组修改特定类别的现有对象的特定属性？

在每种决定委派控制的情况下，将：

- 创建一个允许其执行特定功能的本地组。
- 授予该组在尽可能高的 OU 的特定权限。

注意 要在两个 OU 之间移动对象，执行移动的管理员必须能够在目标容器中创建对象和从源容器中删除对象。由于这些原因，可能需要为可以移动对象的管理员创建一个单独的组，并且授予他们公共的父 OU 的必要权限。

要考虑的对象的列表会随着您部署支持 Active Directory 的应用程序的增多而扩大。但是，有些应用程序将在目录中创建不需要专业管理的对象。例如，运行 Windows 2000 的打印服务器在目录中自动发行打印队列。因为打印服务器负责打印队列对象的管理，所以不必将管理委派到特定的管理组。

通过修改默认计算机容器的 ACL，可以将创建计算机帐户对象的能力委派到所有用户，而不要求管理注意。当用户在默认的计算机容器中的域加入一台计算机时，将创建计算机帐户。

委派每个对象类别控制权限示例

Reskit 公司的汽车部门所在的亚特兰大是两个 Windows NT 4.0 资源域（动力系和底盘）的所在地。Windows 2000 迁移的一部分包括将这两个域合并到 noam.reskit.com 域。

动力系和底盘的管理员现在使用此域：

- 为组成员创建计算机帐户。
- 共享 Windows NT 4.0 备份域控制器 (BDC) 上的文件系统空间，其中到文件系统的访问权限和共享由本地组成员身份控制。

使用委派管理，很容易以 OU 替换资源域。在这种情况下，创建组以管理每种对象，同时给予组对于特定项目的 OU 的完全控制。为防止动力系的管理员操作底盘对象或者相反，特定项目的 OU 是必需的。图 9.15 是这个概念示意图。

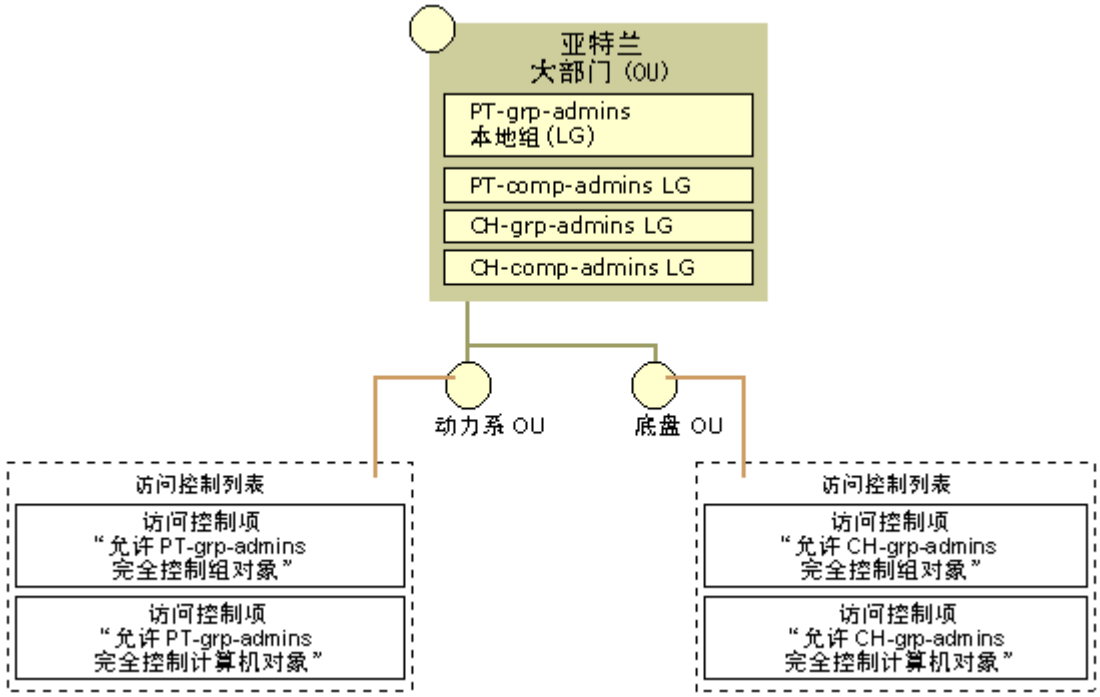


图 9.15 更换资源域

创建 OU 以隐藏对象

即使用户没有读取对象的属性的权利，用户仍然可以通过列出该对象的父容器的内容来看到该对象的存在。隐藏一个对象或一组对象的最简单和最有效的方法是为这些对象创建 OU 并限制具有该 OU 的“列出内容”权利的用户设置。

要创建 OU 以隐藏对象

1. 创建要隐藏对象的 OU。
2. 单击该 OU 的属性页的“安全”选项卡。
3. 从 OU 删除所有的现有权限。
4. 在“高级”对话框中，不选中“从父对象继承权限”复选框。
5. 标识要在 OU 中具有完全控制的组。使用属性页上的“安全”选项卡，给这些组授予完全控制权。
6. 标识那些应该具有普通读访问 OU 和它的目录的组。使用属性页上的“安全”选项卡，给这些组授予读访问权。
7. 标识可能需要特定访问的其他组，例如在 OU 创建或删除特定的对象类别的权利。使用属性页上的“安全”选项卡，给这些组授予特定访问权。
8. 将隐藏的对象移到 OU。

只有那些可以修改 OU 的 ACL 的用户才能用这种方法隐藏对象。

为组策略创建 OU

在 Windows NT 4.0 中，可以使用系统策略编辑器为域中的所有用户和计算机定义用户和计算机配置。使用 Windows 2000，可以使用组策略定义用户和计算机配置，并将这些策略与站点、域或 OU 关联。是否要创建附加的 OU 以支持组策略的应用取决于制定的策略以及所选择的实现方案。有关组策略的详细信息，参见本书中的“应用更改与配置管理”以及“定义客户管理与配置标准”。

在部署后改变 OU 规划

创建新的 OU、在域中移动 OU 子目录树、在同一域的 OU 之间移动对象和删除 OU 非常简单。

移动对象或对象的子目录树将改变这些对象的父容器。从旧的父对象中继承的 ACE 不再应用，可能有从新的父对象中继承的新的 ACE。为避免访问中意外的更改，预先评估将有哪些更改并确定这些更改是否将影响那些正在访问和管理对象的用户。

移动用户对象、计算机对象或者移动包含用户对象或计算机对象的子目录树可以更改应用到这些对象的组策略。为避免客户配置中的意外更改，评估组策略中的更改并确保它们可以为最终用户所接受。

制定站点拓扑规划

Active Directory 站点拓扑是物理网络的逻辑表现。站点拓扑以每个目录林为基础定义。Active Directory 客户机和服务器使用目录林的站点拓扑有效地路由查询和复制通信。站点拓扑也帮助您决定在网络的什么地方放置域控制器。在设计站点拓扑时注意下列主要概念：

站点由速度快、连接可靠的网络组成。

站点定义为一组通过快速、可靠的连接连接起来的 IP 子网。一般而言，具有 LAN 速度或更快速度的网络被认为是快速网络。

站点链接是连接两个或更多站点的窄带的或不太可靠的网络。

站点链接用于模拟两个站点之间的可用带宽的大小。通常，通过一个比 LAN 速度慢的链接连接的任意两个网络被认为是通过站点链接连接。接近容量的快速链接带宽效率低，也可被视为站点链接。站点链接有四个参数：

- 成本

  站点链接的成本大小帮助复制系统决定与其他链接比较后何时使用该链接。成本将决定复制在网络中的路径。

- 复制日程安排

  站点链接有一个相关的日程安排，指出在一天的什么时间链接可用于传送复制通信。

- 复制间隔

  复制间隔指出系统在站点链接的另一面轮询域控制器以复制更改的频率。

- 传输

  用于复制的传输。

客户计算机首先试图与位于同一站点的服务器通信。

当用户开启客户计算机，计算机发送一个消息到该客户机是其成员的域的随机选择的域控制器。这个域控制器根据它的 IP 地址确定该客户位于哪个站点，并将该站点的名称返回到客户。客户将这个信息放入高速缓存并在下次寻找站点中的复制的服务器时使用它。

Active Directory 复制使用站点拓扑产生复制连接。

知识一致性检查器 (KCC) 是一个内置的进程，该进程创建和维护域控制器之间复制连接。站点拓扑信息用于指导这些连接的创建。调整站点内的复制以使复制反应时间缩小到最短，调整站点之间的复制以使带宽使用程度最低。表 9.1 是站点内和站点之间复制的差别。

表 9.1 站点内与站点之间复制

站点内复制	站点之间复制
复制通信没有压缩以节省处理器时间。	复制通信压缩以节省带宽。
当更改需要复制时复制伙伴互相通知以减少复制反应时间。	当更改需要复制时复制伙伴不互相通知以节省带宽。
复制伙伴按时间段互相轮询更改情况。	复制伙伴在指定的时间间隔内互相轮询更改情况，只在安排好的时间段内进行。
复制使用远程过程调用 (RPC) 传输。	复制使用 TCP/IP 或 SMTP 传输。
复制连接可以在位于相同站点的任意两个域控制器之间创建。 KCC 使用多个域控制器创建连接以减少复制反应时间。	复制连接仅在两个桥头服务器之间创建。 站点中的每个域的域控制器被 KCC 指定为桥头服务器。桥头服务器为该域处理所有的站点之间复制。 KCC 根据站点链接成本，使用成本最少的路径在桥头服务器之间建立连接。如果低成本路径中所有的域控制器无法实现，KCC 将只能通过高成本路径的创建连接。

站点拓扑信息保存在配置容器中。

站点、站点链接和子网都保存在配置容器中，该配置容器复制到目录林中的每个域控制器中。目录林中的每个域控制器完全掌握站点拓扑的情况。对站点拓扑的更改会复制到目录林中每个域控制器中。

注意 站点拓扑是单独的，与域层次结构没有关系。一个站点可以包含很多域，一个域可以出现在很多站点中。

站点拓扑规划过程

要为目录林创建站点拓扑，按下面的过程进行：

- 以物理网络拓扑作开始点，定义站点和站点链接。
- 将服务器放置在站点中。
- 弄清部署后对站点拓扑的更改将如何影响最终用户。

在制定站点拓扑规划时，很可能需要咨询：

- 管理和监视网络上的 TCP/IP 实现的组。
- 目录林中每个域的域管理员。

有关站点或本节中讨论的任何主题的详细信息，参见 *Distributed Systems Guide*。

定义站点和站点链接

要为目录林创建站点拓扑，必须获得网络的物理拓扑并根据可用带宽和网络可靠性创建更通用的拓扑。

如果在制定域规划时进行物理分区，可以使用使用站点拓扑和创建的域控制器放置规划作为站点拓扑的开始点。如果跳过了在本章前面的物理分区作业，建议您查看“ 确定每个目录林中域的数量 ”并立即创建一个基本站点拓扑。

在创建站点拓扑时，有一个网络的物理拓扑布局图将会对您很有帮助。该图应该包含网络的物理子网的列表、媒体类型和每个网络的速度以及每个网络之间的互相连接。

建立站点

首先，创建网络上站点的列表。

- 创建一个站点，以包括高速骨干网连接的每个 LAN 或每组 LAN，并给站点的名称。站点的连接必须可靠并且始终可用。
- 为每个没有直接连接到网络的其他部分并只能通过 SMTP 邮件到达的位置创建一个站点。
- 确定哪些站点没有本地域控制器，并将这些站点与其他邻近的站点合并。站点帮助有效地路由客户到域控制器和域控制器到域控制器通信。没有站点中的域控制器，就没有到站点的复制通信可控制。

对于每个添加到规划的站点，记录组成站点的 IP 子网组。以后在目录中创建站点时将需要该信息。

注意 站点名称在 DNS 中注册的记录中被域定位器使用，所以它们必须是合法的 DNS 名称。建议在站点名称中只使用标准字符 A–Z、a–z、0–9 和连字符 (–)。

记住，客户在试图与其他站点的域控制器通信之前，将尽量与客户所在的相同站点的域控制器通信。任何时候一组网络之间的带宽都已足够，不需考虑一个网络上的客户是否与不同网络上的服务器通信，因而可以所有的网络当作在一个站点中一样。

如果客户在一个未在目录中定义的子网中，那么不认为它是站点的一部分，并从一个特定域的所有域控制器中随机选择。可能会遇到这样的情况，并非所有的子网都在目录中定义，例如当新的子网添加网络中时。要将这些客户与站点相关联，创建两个表 9.2 中所示的默认子网，然后将它们与站点相关联。

表 9.2 默认子网

子网 ID	掩码	说明
128.0.0.0	192.0.0.0	捕获还未在目录中定义的 B 类网络上的所有客户。
192.0.0.0	224.0.0.0	捕获还未在目录中定义的 C 类网络上的所有客户。

对于 A 类网络上的客户没有默认子网。

任何时候两个网络都被链接分开，这些链接在一天的部分时间使用频繁而在其余的时间是空闲的，将这些网络放入不同的站点。可以安排站点之间的复制的时间以防止复制通信与高峰使用时间内的其他通信争用。

如果整个网络由快速的、可靠的连接组成，整个网络可以被视为是一个站点。

使用站点链接连接站点

接下来，使用站点链接连接站点以反映网络的物理连接。为每个站点链接取一个名称。

站点链接是可传递的，所以如果站点 A 连接到站点 B，站点 B 连接到站点 C，那么 KCC 认为站点 A 中的域控制器可以与站点 C 中的域控制器通信。如果事实上在站点 A 和站点 C 之间存在一个截然不同的网络连接，只需在这两个站点之间创建一个站点链接。

对每个创建的站点链接，记录下列信息：

- 复制日程安排

  复制轮询仅在确定的时间段或七天以上间隔内发生。链接上的默认日程安排允许复制轮询在七天间隔期间发生。

- 复制间隔

  当日程安排允许复制时，复制轮询以特定的间隔发生。默认轮询间隔是三个小时。

- 复制传输

  如果站点仅可以通过 SMTP 到达，选择 SMTP 传输。否则，选择 TCP/IP 传输。

- 链接成本

  分配每个站点链接的成本以反映可用带宽或与其他站点链接相比较的带宽成本。

连接许多站点的骨干网络可以用一个连接许多站点的站点链接表示，而不需创建几个站点之间的链接网。如果许多链接具有相同的特性，这是一个减少需要创建和管理的站点链接数量的好办法。图 9.16 说明了一个连接四个办公室的帧中继网络如何表示成单个链接，代替六个单独的链接的网的方法。

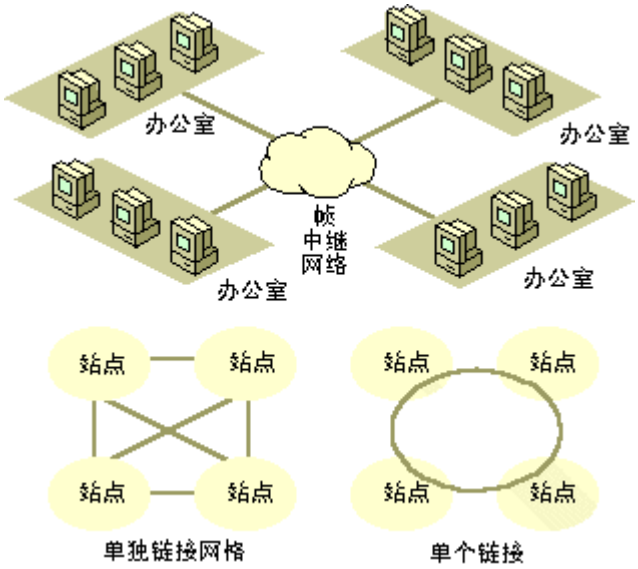


图 9.16 单个链接或链接的网

注意 复制日程安排决定域控制器何时轮询复制伙伴发生更改的情况。如果计划的窗口关闭时复制周期仍在进行，复制继续直到当前的周期完成。

图 9,17 是 Reskit 公司的站点拓扑图。站点命名规则使用区域代码、最近的机场的代码和标识号码的组合。站点链接名称包含连接的站点的名称。

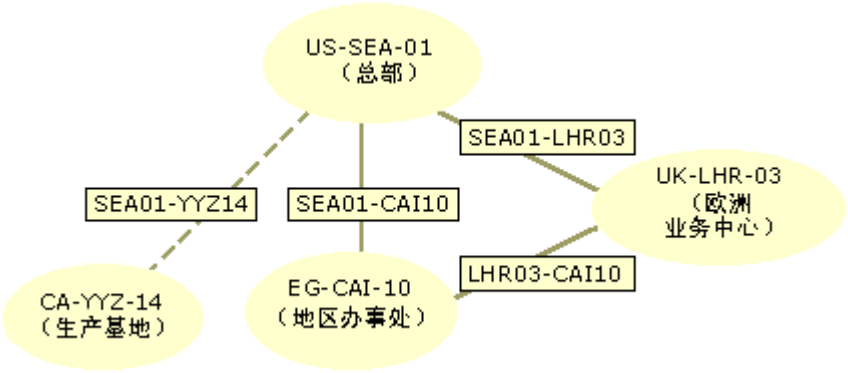


图 9.17 Reskit 公司站点拓扑

表 9.3 显示了 Reskit 站点拓扑中的每个站点链接的参数。

表 9.3 Reskit 站点拓扑的站点链接参数

站点链接	传输	成本	轮询间隔	日程安排
SEA01-YYZ14	SMTP 协议	100	30 分钟	每天 0500 到 0900 UTC
SEA01-CAI10	IP	100	30 分钟	每天 2000 到 0400 UTC

SEA01-LHR03	IP	25	1 小时	（始终）
LHR03-CAI10	IP	50	15 分钟	每天 2000 到 0400 UTC

复制仅在生产工厂和总部之间的链接的高峰以外的时间发生。复制也安排在地区办公室和其他站点之间的高峰以外的时间发生。因为地区办公室和运行中心之间的链接开销低于地区办公室和总部之间的链接开销，KCC 在与总部的桥头连接之前试图与运行中心的桥头连接。总部和运行中心之间的链接的日程安排是相对宽松的，但使用较长的轮询间隔以减少通信。

在站点中放置服务器

站点拓扑中服务器的位置对 Active Directory 的可用性有直接的影响。在域规划的物理分区过程中，为域控制器放置创建一个基本规划。通过将服务器放置到站点拓扑，将完成这个规划的细节。

放置附加的域控制器

在分区过程中，您决定了哪些站点中的每个域都有域控制器，但是并不能决定每个站点中的每个域放置的域控制器的数量。为一个特定域创建的域控制器的数量取决于两个因素：容错要求和负载分布要求。

对于每个域，使用下列指导方针决定是否需要更多的域控制器：

总是至少创建两个域控制器。即使是用户数量较少的小型域，至少也要创建两个域控制器，这样域就没有单个故障点。

对于包含单个域控制器的每个站点，决定是否信任 WAN 的故障转移。如果单个域控制器出现故障，可以由位于其他站点中那个域的域控制器服务站点中的客户。如果网络连接不太可靠或间歇可用，可能不能信任网络处理故障转移。在这种情况下，在站点中为该域放置第二个域控制器。

在站点中为域放置更多的域控制器以处理客户工作量。一个特定的服务器可以处理的客户的数量取决于工作量和服务器的硬件配置。客户从站点中的可用域控制器中随机选择以均匀地分配客户负载。

放置全局编录服务器

全局编录服务器的有效性对于目录的运行是很关键的。例如，当为本机模式域处理用户登录请求时或当用户使用用户主要名称登录时，必须有一个全局编录服务器可用。

注意 当为本机模式域中的用户处理登录请求时，域控制器给全局编录服务器发送一个查询到以判断用户的通用组成员身份。因为可以明确拒绝组对资源的访问，所以为正确执行访问控制，必须完全知道用户的组成员身份。如果当用户要登录时，本机模式域的域控制器不能联系到全局编录服务器，则域控制器拒绝登录请求。

通常，至少在每个站点中指定一个域控制器作为全局编录服务器。

使用用于单独的域控制器的相同故障转移和负载分配规则决定是否需要在每个站点中增加全局编录服务器。

注意 在单个域环境中，不要求全局编录服务器处理用户登录请求。但是，仍然应该使用所建议的步骤指定全局编录服务器。客户在搜索操作时仍然寻找全局编录服务器。同时，将全局编录服务器准备就绪使得在以后添加更多的域时，系统更容易适应。

放置 DNS 服务器

DNS 的可用性直接影响 Active Directory 的可用性。客户依赖 DNS 来查找域控制器，而域控制器依赖 DNS 来查找其他的域控制器。即使现在已在网络中部署了 DNS 服务器，可能需要调整服务器的数量和位置以满足 Active Directory 客户和域控制器的要求。

通常，至少在每个站点中放置一个 DNS 服务器。站点中的 DNS 服务器应该负责站点中域的定位器记录，这样客户不需要离站查询的 DNS 服务器即可确定站点中的域控制器的位置。域控制器也将定期验证主服务器上的每个定位器记录项目是否正确。

一个满足所有要求的简单配置是使用集成 Active Directory 的 DNS 将域的定位器记录保存在域中，并为那些域控制器出现的每个站点在一个或多个域控制器上运行 Windows 2000 DNS 服务。

分发目录林内定位器记录

目录林中的每个域控制器注册两组定位器记录：一组特定域记录，以 *<DNS-domain-name>* 结束，一组目录林内记录，以 *_msdcs.<DNS-forest-name>* 结束。目录林内记录引起来自目录林的所有部分的客户和域控制器的注意。例如，全局编录定位器记录和复制系统用来确定复制伙伴位置的记录都包含在目录林内记录中。

对于要互相复制的任何两个域控制器，包括相同域的两个域控制器，必须能够查寻目录林内定位器记录。为了使一个新创建的域控制器参与复制，它必须能够在 DNS 中注册它的目录林内记录，而其他的域控制器必须能够查寻这些记录。由于这个原因，使目录林内定位器记录对于每个站点的每个 DNS 服务器可用是很重要的。

要做到这一点，创建一个称为 *_msdcs.<DNS-forest-name>* 的单独区域，并将该区域复制到每个 DNS 服务器。如果使用简单的集成 Active Directory 的配置，可以将目录林根域中的这个区域的主副本放置在 *<DNS-forest-name>* 区域。然后可以使用标准 DNS 复制将该区域复制到域以外的 DNS 服务器。

通常，仅将该区域复制到每个站点的一个 DNS 服务器是不够的。如果一个 DNS 服务器没有 *_msdcs.<DNS-forest-name>* 区域的本地副本，它必须使用 DNS 递归以查寻该区域中的一个名称。对于执行递归的 DNS 服务器，它联系负责名称空间的根的 DNS 服务器（DNS 根服务器）并继续 DNS 中的委派，直到它找到出所需记录。如果站点中没有 DNS 根服务器，而且该站点和其他站点之间的链接已断开，DNS 服务器不能执行递归。因此，找不到负责 *_msdcs.<DNS-forest-name>* 的 DNS 服务器，即使这些 DNS 服务器在相同的站点。

DNS 客户配置

客户和域控制器应该使用至少两个 DNS 服务器 IP 地址配置：一个首选本地服务器和一个备用服务器。备用服务器可以在本地站点，或者如果信任网络处理故障转移，也可以是远程的备用服务器。

部署后更改站点拓扑

目录林站点拓扑非常灵活并且在最初部署之后容易更改。随着物理网络的发展，记住评估并调整站点拓扑。由于网络的更改增加或减少带宽或可靠性，记住创建或删除站点和站点链接，并确信调整站点链接参数以平衡复制反应时间与带宽使用程度。

在对站点拓扑进行更改之前，预计该更改对可用性、复制反应时间和复制带宽的影响以及这将如何影响最终用户。因为站点拓扑保存在配置容器中，更改将复制到目录林中的每个域控制器中。对站点拓扑的频繁更改将引起大量的复制通信，应该进行次数较少的、大型的更改，而不是进行次数很多的、小型的更改。根据复制拓扑和日程安排，站点拓扑更改可能耗费较长的时间才能到达目录林中的每个域控制器。

设计 Active Directory 结构规划任务列表

使用表 9.4 作为检验表以确保执行完设计 Active Directory 结构所必需的所有主要任务。

表 9.4 Active Directory 规划任务列表

任务	所在章节
确定目录林的数量。	制定目录林规划
为每个目录林制定更改控制策略。	制定目录林规划
确定每个目录林中域的数量。	制定域规划
选择目录林根域。	制定域规划
给每个域取一个 DNS 名称。	制定域规划
规划 DNS 服务器部署。	制定域规划
用快捷信任关系优化身份验证。	制定域规划
创建 OU 以委派管理。	制定部门规划
创建 OU 以隐藏对象。	制定部门规划
为组策略创建 OU。	制定部门规划
定义站点和站点链接。	制定站点拓扑规划。
在站点中放置服务器。	制定站点拓扑规划

第 10 章 - 确定域迁移策略

要成功地从 Microsoft® Windows NT® 3.51 和 Microsoft® Windows NT 4.0 迁移到 Microsoft® Windows® 2000 要求仔细分析当前系统并深入地规划。参加升级过程逻辑设计的网络工程师必须熟悉推荐的配置和本章所介绍的步骤。虽然这些推荐也适用于较小的单位，但本章强调的重点是针对至少具有 2,500 台个人计算机的单位。

因为本章的重点是规划域升级和重组，以及通过升级 Windows NT 域规划 Microsoft Active Directory™ 目录服务名称空间，大多数 Active Directory 名称空间规划必须首先完成。另外，作为本章的先决条件，您需要熟悉下列内容：可在 Windows 2000 中部署的功能、本单位的部署目标、本单位的当前域模型，以及当前网络配置的硬件和软件清单。

本章内容

开始迁移规划过程
规划域升级
规划域重组
域迁移工具
迁移规划任务列表

本章目标

- 本章将帮助您撰写下列规划文档：
- 迁移项目线路线
- 修订 Active Directory 名称空间规划文档
- 域迁移规划

资源工具包中的相关信息

- 有关 Active Directory、域名系统 (DNS) 名称空间设计、站点拓扑或组的详细信息，参见本书的“设计 Active Directory 结构”。
- 有关 Windows 2000 Server 自动安装的详细信息，参见本书的“服务器自动安装与升级”。
- 有关 Windows 2000 Professional 自动安装的详细信息，参见本书的“客户机自动安装与升级”。

开始迁移规划过程

在进行域升级或重组之前，弄清规划过程是很重要的。

备注 本章所介绍的步骤和建议基于非复制计算机的升级。只有运行 Windows NT Server 3.51 和 Windows NT Server 4.0 的计算机才能升级到 Windows 2000 Server。旧的版本不能升级到

Windows 2000 Server。在本章中，术语“Windows NT”表示 Windows NT Server 的 3.51 和 4.0 两种版本。

规划过程阶段

迁移域的规划过程包括下列阶段：

1. 设计 Windows 2000 目录林。有关如何设计 Windows 2000 目录林的信息，参见本书的“设计 Active Directory 结构”。
2. 规划从 Windows NT 域到 Windows 2000 本地域的迁移和部署 Windows 2000 Server 的新功能。
3. 规划 Windows 2000 域的重组。

   本阶段可能不必要，也可能将来合适，这取决于本单位的要求。有关如何重组域的详细信息，参见本章稍后的“规划域重组”。

图 10.1 说明了迁移到 Windows 2000 Server 的主要步骤。本章将详细说明每一个步骤，从最初规划阶段到域升级和重组的具体任务。

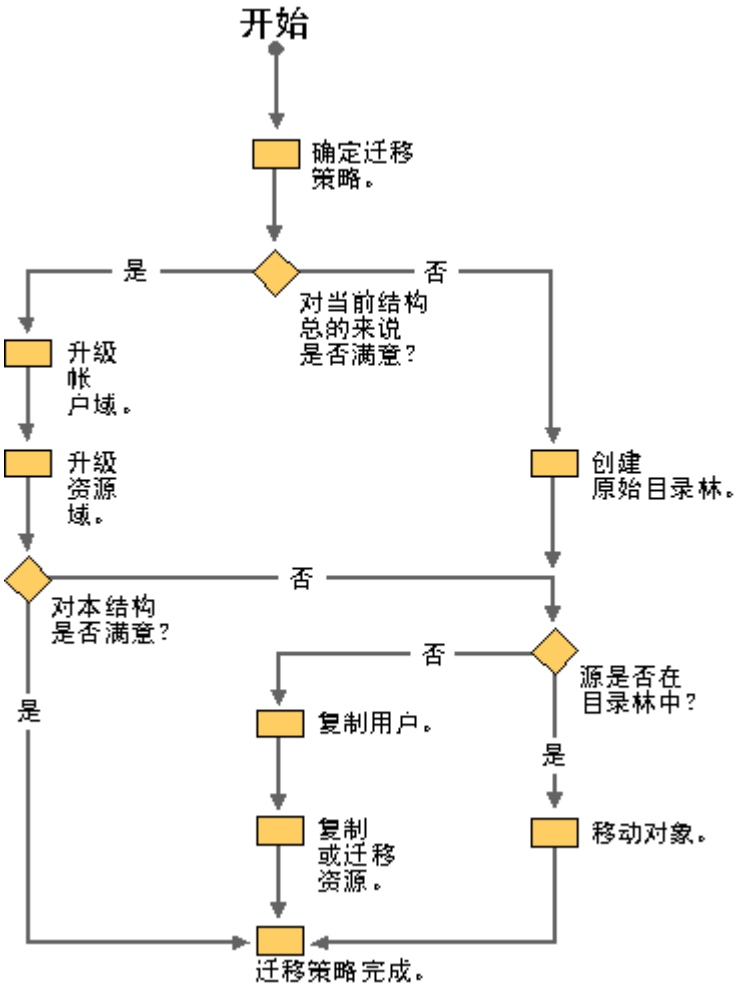


图 10.1 迁移规划流程图

确定迁移路线图

在任何规划过程中做出重要的决定并使之完善是通常的做法。在规划迁移的过程中所做的选择可能会使您将一些系统功能的部署推迟到晚些时候。制定迁移路线图的第一步是明确迁移目标并将它们按优先次序排好，并弄清您做的选择的含意。

在选择迁移到 Windows 2000 的过程中，无疑您已明确您渴望部署的某些功能和优点。下面一节列出了一些典型的迁移目标并解释了这些目标的关键概念和它们的含意。在读完本节之后，您应有足够的信息完成迁移项目路线图。

迁移目标

迁移规划必须反映主要迁移目标。这些目标可能是与业务有关的，也可能与迁移本身有关。

在大多数情况下，与业务有关的目标促进最初的迁移决定。此类目标的例子包括更高的可扩展性和改进的安全性。在作出实施选择时要涉及与业务有关的目标，这些目标可用于评估各种方案的利弊。通常会准备某种形式的符合性表格，这些表格在以后阶段用于明确在最后的平台上待实现的技术和产品功能。这些技术和功能将帮助您实现业务目标。

与迁移有关的目标可包括下列考虑因素：损坏对生产系统的影响、最终系统性能和延长平均无故障时间的方法。这些目标可以决定如何制定测试规划和接受标准。

与迁移有关的目标不受实现 Windows 2000 Server 具体技术功能这一需要的影响，但更加注重迁移过程本身。表 10.1 列出了一些与迁移有关的目标。

表 10.1 与迁移有关的目标

目标	在迁移过程中的含义
使对生产环境的损坏最小化	用户对数据、资源、和应用程序的访问在迁移时和迁移后需要维持。 迁移时和迁移后用户熟悉的环境需要维持。
维持系统性能	用户对数据、资源、和应用程序的访问在迁移时和迁移后需要维持。 迁移时和迁移后用户熟悉的环境需要维持。
延长平均无故障时间	用户对数据、资源、和应用程序的访问在迁移时和迁移后需要维持。 迁移时和迁移后用户熟悉的环境需要维持。
使管理的开销最小化	必须无缝迁移用户帐户。
	若有可能，用户必须能够保留他们的密码。
	管理员访问客户计算机的次数减到最少。
	只需安装最少的新的资源使用权限。
使“ quick Wins ”最大化	企业需尽早使用新平台的关键功能。
维护系统安全	对安全策略的影响最小。

为了从 Windows 2000 技术获得最大利益并实现迁移目标，建议尽快地将 Windows 2000 域切换到本机模式。然而，视现有的网络配置，您可能在从域中完全消除 Windows NT 备份域控制器 (BDC)

以前不能切换到本机模式。有关“ 本机模式 ”的定义，参见本章稍后的“ 确定切换到本机模式的时间 ”。

备注 读者仍可以在升级域基础结构之前部署 Windows 2000 客户机和成员服务器。参见本章稍后的“ 升级客户机和服务器 ”。

迁移的概念

有两个方法实现想要的基础结构:

- 域升级 - 有时称为“ 就地升级 ”或“ 升级 ”。

  “ 域升级 ”是将 Windows NT 域的主域控制器 (PDC) 和 BDC 从 Windows NT Server 升级到 Windows 2000 Server 的过程。

- 域重组 - 有时称为“ 域合并 ”。

  “ 域重组 ”是整个域结构的重新设计，通常产生较少的、更大的域。这种选择适用于那些对当前域结构不满意的人或那些觉得升级必将严重影响生产环境的人。

升级和重组不是互斥的，一些单位可能先升级然后重组，而一些单位可能一开始就进行重组。这两种情况都要求在作出选择之前仔细考虑和规划。

升级客户机和服务器

虽然本章的重点是域升级和重组，但这并不意味着读者必须将 Windows 2000 客户机和成员服务器的部署推迟到将域基础结构升级之后。您可以使用现有的 Windows NT 环境中的 Windows 2000 客户机和服务器，但仍能从新的技术中获益匪浅。表 10.2 列出了一些将客户机和服务器升级到 Windows 2000 直接获得的好处。

表 10.2 简单客户机或服务器升级的优点

优点	功能
易管理性	即插即用
	设备管理器中的硬件向导
	支持通用串行总线
	Microsoft 管理控制台
	新的备份工具
安装和故障诊断工具	自动应用程序安装允许管理员指定一组用户或用户组始终可以使用的应用程序。如果需要的应用程序必要时不可用，它会自动安装在系统中。
文件系统支持	NTFS 5.0 增强功能包括磁盘配额支持，整理目录结构碎片功能，和压缩网络 I/O
	FAT32
应用程序服务	Win32® Driver Model

	DirectX®5.0
	Windows Script Host
信息共享和发布	用于 Windows 2000 Server 的 Microsoft 分布式文件系统 (Dfs) 使用户查找和管理网络中的数据更容易。
	集成的 Internet Shell
打印服务器服务	通过 Active Directory Printing 从 Internet 定位打印机更容易
可扩展性和可用性	改进的对称多处理器支持
安全性	加密文件系统

域迁移的注意事项

本节将向您逐步介绍用于任何迁移的重要规划和准备活动。您自己的规划过程将决定准确的步骤，但是下面几节将重点介绍必须考虑的事项。

升级决定

当确定如何升级域时，考虑下列问题：

- 升级是否对您合适？

  如果下列条件中的一些或全部都为真的话，您可能回答“是的”：

- 您对当前域结构满意。

- 您对大部分域结构满意，可以分两阶段迁移:升级到 Windows 2000，然后重组以解决任何问题。

- 您觉得您能管理迁移，不会影响生产环境。

- 需要以什么顺序升级？

  答案取决于是指升级域控制器的顺序还是升级域的顺序:

- 需要以什么顺序升级域控制器？

  在域内部，升级的顺序很简单。须先升级 PDC，但要注意可能出现的复杂局面，比如在要升级的域中，与存放导出目录的 PDC 一起使用 LAN 管理器复制服务。在这种情况下必须在升级 PDC 之前改变导出目录宿主。有关 LAN 管理器复制的详细信息，参见本章稍后的“LAN 管理器复制服务过程”。

- 需要以什么顺序升级域？

  如果先升级帐户域，您会发现管理和委派更容易。然后需要升级资源域。

- 需要以什么顺序升级服务器和客户机？

可以在任何时候升级服务器和客户机。这不取决于 Windows 2000 基础结构。

- 何时需要将域切换到本机模式？

  必须尽快将域切换到本机模式以便能使用 Windows 2000 的全部功能，比如更好的目录可扩展性，通用和域本地组，和组嵌套。

备注 只有升级所有的域控制器之后才能将域切换到本机模式。

重组决定

当确定是否及如何重组域时，应考虑下列问题：

- 需要重组吗？

  如果下列条件中的一些或全部都为真的话，您可能回答“是的”：

- 您对大部分域结构满意，可以分两阶段迁移:升级到 Windows 2000，然后重组以解决任何问题。

- 您对当前域结构不满意。

- 您觉得迁移必将影响生产环境。

- 何时需要重组？

  答案取决于重组的理由。

- 如果您可以通过两阶段迁移解决迁移要求，那么需要在升级之后重组。

- 如果您觉得域结构不能恢复(例如，如果您决定必须重新设计目录服务基础结构以便利用 Active Directory 的增强功能)，必须在迁移过程开始的时候重组。

- 如果您觉得不能避免对生产环境的影响，必须在迁移过程开始的时候重组。

备注 建议在完成升级之后但在使用应用程序部署或新的组策略等功能之前重组。如果在使用了一些功能之后重组，比在迁移过程开始的时候进行重组困难得多。

应用程序兼容性

在决定如何全面执行域迁移之后，确定业务应用程序是否与 Windows 2000 兼容非常重要。本步骤对部署的成功至关重要，必须在决定如何以及何时迁移应用程序服务器之前完成。在明确了策略应用程序之后，一定要将它们包括在测试规划中。所有的策略应用程序必须在迁移过程之前测试。有关迁移应用程序服务器的详细信息，参见本书的“升级和安装成员服务器”。

有关应用程序的一些重要问题包括:

- 应用程序是否运行于 Windows 2000？

  如果答案是“不”，那么对于升级规划可能涉及其它一些问题。

- 应用程序是否需要运行于 BDC？

  如果答案是“是的”，并且应用程序不运行于 Windows 2000，那么将升级的域切换到本机模式将非常困难。

- 您与应用程序软件供应商是否有联系？

  如果发现应用程序在 Windows 2000 上运行出现问题，必须知道应用程序供应商计划如何支持 Windows 2000。

- 如果应用程序是内部开发的，是否计划开发 Windows 2000 版本？

  如果应用程序不能运行于 Windows 2000，必须知道提供 Windows 2000 支持的所有计划。

- 在客户机和服务器上部署的什么操作系统?

  此问题的答案对于迁移途径有密切关系。某些软件到 Windows 2000 的升级路径不受支持（例如，从 Windows NT 3.5）。

备注 您可能不希望在资源域中维护 Windows NT 3.51 服务器，因为 Windows NT 3.51 不支持通用或域本地组成员身份。Windows NT 3.51 不识别面向在 Windows 2000 域之间移动的用户帐户的 SIDhistory 功能。

知道这些问题的答案有助于制定涵盖重要测试案例的测试规划。还有助于开发项目风险评估，以搞清无法正常工作的各种应用程序的相关问题，包括任何建议的解决办法。

有关测试业务应用程序的详细信息，参见本书的“测试应用程序与 Windows 2000 的兼容性”。

备注 一些 Windows NT 为设计的应用程序服务，比如 Windows NT 路由和远程访问服务 (RRAS)，采用未进行身份验证的用户帐户信息访问。Active Directory 的默认安全权限不允许对帐户信息进行无身份验证的访问。Active Directory 安装向导通过提供附加权限，允许为兼容性配置 Active Directory 安全性。如果您觉得放松 Active Directory 的安全，允许使用 RRAS 服务器会危害安全策略，那么需要先升级这些服务器。

如果使用 LAN 管理器复制服务复制域内部的脚本，那么必须最后升级存放导出目录的服务器。

互操作性要求

下一步是考虑 Windows 2000 系统需要与传统 Windows 系统和非 Microsoft 操作系统相互操作的程度。如果您计划维护包括 Windows 2000 之外的网络操作系统的异类环境，必须确定哪些传统应用程序和服务应保留或升级，以便在所有平台上保留可接受的功能。

互操作性注意事项有两个方面：

- 在异类环境中的互操作性要求有哪些？

  这包括迁移的环境必须与其他操作系统和网络服务相互操作的程度。

  重要的注意事项包括：

- 必须维护 Windows 2000 之前的客户机，这意味着必须维护诸如 Windows Internet 命名服务 (WINS)的服务，以便支持名称解析。
- 必须维护 Windows 2000 之前的域，这意味着必须维护和管理显式信任。
- 必须与非 Microsoft 操作系统相互操作，比如 UNIX。这是迅速迁移以便广泛使用 Kerberos 身份验证的一个原因。

- 对源环境的互操作性要求有哪些？(从何处迁移？)

管理过渡期的环境是一个非常复杂的任务，必须象下面几节所介绍的那样仔细规划。

Active Directory 对象的磁盘存储要求

在迁移规划的早期，考虑需要多少磁盘空间储存 Active Directory 必需的对象非常重要。所必需的总磁盘空间取决于 Windows 2000 目录林的大小。有关设计此目录林的信息，参见本书的“设计 Active Directory 结构”。

表 10.3 是每一种类型的 Active Directory 对象的磁盘空间要求。

表 10.3　Active Directory 对象所要求的磁盘空间

对象	所要求的磁盘空间(字节)
用户对象	3.6K
部门 (OU) 对象	1.1K
属性(10 字节)	100
公钥证书 (Windows 2000 证书服务颁发的 X.509 v3 证书)	1.7K

规划域升级

在考虑了与域迁移有关的问题并制定解决问题的规划之后，就可以开始规划实际的升级过程了。

备注 必须在计划升级之前完成 Windows 2000 目录林的设计。有关设计此目录林的信息，参见本书的“设计 Active Directory 结构”。

“域升级”是将 Windows NT 域的主域控制器 (PDC) 和 BDC 从 Windows NT Server 升级到 Windows 2000 Server 的过程。升级是迁移办法中最容易和风险最小的的方法，因为它能保留大多数系统设定、首选项和安装的程序。

因为 Windows 2000 Server 以全面的互操作性支持混合网络，因此不必升级域中的所有服务器便可利用 Windows 2000 功能。考虑将升级到 PDC 作为过程的第一阶段，这样通过升级 BDC，再升级成员服务器您将获得额外的、意想不到的好处。

因为迁移涉及操作系统升级而不是新的安装，所以虽然在过程中启用 Windows 2000 功能，但现有的域结构、用户、和组得以保留。当您完成升级并能使用高级 Windows 2000 管理工具和功能时，可能考虑对域进行重组。然而要注意，域重组不是一件轻松的任务。如果结构改变是目标之

一，应考虑在最初的迁移阶段而不是在升级之后进行域重组。但应在采取行动之前反复斟酌这两种方案。

域升级将完成下列工作：

- 通过现有的 Windows NT 信任关系维护 Windows NT 域的访问权。
- 维护 Windows NT 服务器以及 Windows 95 和 Windows 98 客户机的访问权。此访问权对客户计算机上的客户是透明的。
- 维护用户帐户密码，允许用户使用相同的密码登录到相同的帐户域。

当规划升级时，您需要：

- 确定支持哪些升级路径。
- 检查现有的域结构。
- 制定恢复规划。
- 确定升级域的顺序。
- 确定升级域控制器的策略。
- 确定切换到本机模式的时间。

备注 不必在升级客户机之前将服务器基础结构升级到 Windows 2000 Server。甚至可以在升级域控制器之前升级客户机和成员服务器，但在升级域控制器之前您不能使用 Active Directory 的功能。

确定支持的升级路径

当规划升级时，必须确定当前操作系统是否能直接升级到 Windows 2000。 表 10.4 列出了当前支持的升级路径。如果发现不支持直接升级操作系统，必须先升级到 Windows 95 或 Windows 98（客户机），或升级到 Windows NT （客户机和服务器）。要确保此中间步骤反映在升级规划中。

有关升级成员服务器的详细信息，参见本书中的“ 安装与升级成员服务器 ”。

表 10.4 支持的升级路径

操作系统	升级到 Windows 2000 Professional	升级到 Windows 2000 Server
Windows 3.x	否	否
Windows NT 3.1	否	否
Windows NT Workstation 3,51	是	否
Windows NT Server 3,51	否	是
Windows 95 和 Windows 98	是	否
Windows NT Workstation 4.0	是	否
Windows NT Server 4.0	否	是

检查现有域结构

在确信当前操作系统可以升级到 Windows 2000 之后，下一任务是检查现有的域结构。为帮助您理解所讨论的概念，看看图 10.2 所示的 Windows NT 域结构。本例是根据许多单位的域设计所作出的。多主域模型。本例显示以帐户域开始的升级，帐户域通常是第一个要升级的域。

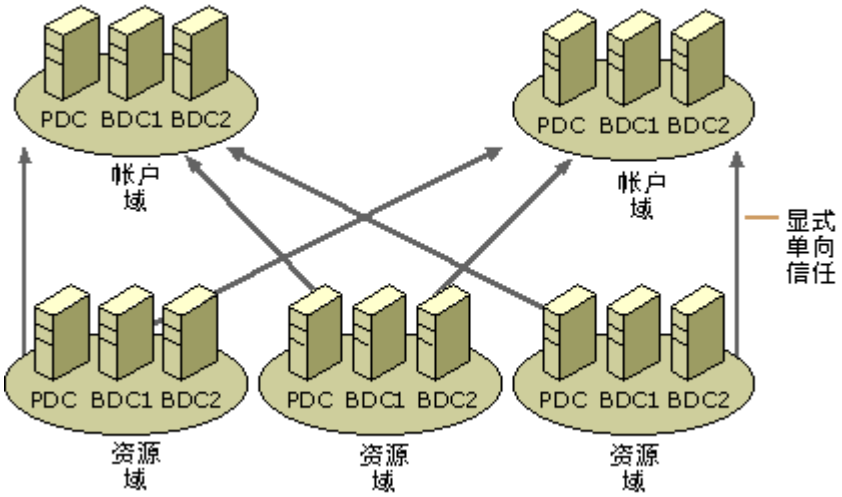


图 10.2 多主域模型示例

当检查现有的 Windows NT 域结构时，应注意下列问题：

- 您的域结构类型是什么？

  现有的域结构有助于确定如何规划域升级。

- 是否已有信任关系(单向的和双向的）以及不想包括在目录林中的域？

  这些 Windows NT 域使用显式单向信任连接到目录林。升级到 Windows 2000 Server 并作为相同的目录林组成部分的域将通过可传递双向信任连接。这是知道哪些信任必须保持显式为什么非常重要的原因。注意升级之前的所有现有信任都将保留。

- 有多少域控制器，以及在每个域内的什么位置？

  此信息将有助于算出升级某一指定域需要的工作量。

- 本单位有哪些 DNS 名称空间？

  因为不能在 Windows 2000 中更改域名，必须知道本单位正在使用的现有名称空间以及本单位允许哪些额外的名称空间，以便您能为目录林创建唯一的名称空间。

制定恢复规划

制定恢复规划防止升级时发生意外的数据损失是很重要的。此规划必须详细列出如何备份域控制器、应用程序和其它数据。规划是否彻底将决定您能否完全地恢复到原始配置，有时甚至能决定

是否到达无法挽回的地步。在制定恢复规划时，应确定是否有一个增量迁移可以停止、完全迁移可以开始的点。

在执行迁移之前应完成以下几个任务：

- 将 BDC 添加到所有只包含单个域控制器 - PDC 的 Windows NT 域。这将保证在升级到 PDC 失败时域不会成为孤立的。
- 确定诸如文件和打印服务或动态主机配置协议 (DHCP) 的服务是否在 PDC 和 BDC 中运行。

  将这些服务备份到磁带中，并测试备份磁带。
- 将所有的 BDC 与 PDC 完全同步。

  在将 PDC 和其它 BDC 升级到 Windows 2000 Server 之前将一个 BDC 脱机。作为测试，在开始迁移之前执行以下几个步骤：

  1. 将脱机 BDC 提升到 PDC 并检查数据。
  2. 使此 PDC 在迁移之后保持脱机和可用，并确保其余的 BDC 定期备份。

  警告 在脱机 PDC 保持脱机状态时跟踪对域的所有的更改(例如，新的帐户和密码更新)。如果 Windows 2000 域控制器发生灾难，必须回退到脱机 PDC。如果在脱机 PDC 保持脱机状态时没有跟踪所有的域更改，那么在脱机 PDC 将数据复制到 BDC 时这些更改就会丢失。注意重建的帐户有不同的安全标识符 (SID)，因此，它们可能无法使用某些资源。

  对于图 10.1 中的流程图中的每一步，回答以下几个问题：

  3. 如何将系统回退到恢复状态？
  4. 需要什么管理工具才能完成升级和恢复状态？

管理到 Windows 2000 目录林的过渡

作为域升级规划的组成部分，必须认真地管理您设计的到 Windows 2000 目录林的过渡。一定要记住以下几个注意事项：

- 正确定义目录林名称空间。如果不，则必须将目录林重组到正确的名称空间。
- 认真地创建目录林的根域。在创建根域之后，便不能更改。
- 认真地创建子域。如果您将子域加入到目录林错误部分，您将不得不执行重组，而这不是您规划的组成部分。
- 确定诸如有关组和访问控制表 (ACL) 使用的、不妨碍未来规划的策略。

有关设计 Windows 2000 目录林的详细信息，参见本书的“设计 Active Directory 结构”。

考虑资源域的升级

如果您进行就地升级，可能考虑升级资源域。资源域用于 Windows NT，以保存服务器和客户计算机之类资源的计算机帐户。资源域主要用于：

- 限制帐户数据库的大小。

  在 Windows NT 中，推荐的安全帐户管理器 (SAM) 帐户数据库最大为 40 MB。在包含用户帐户、安全组、和 Windows NT 客户和服务器帐户的域中，这可能相当于不足 20,000 个用户帐户。为规划超出这个数字的单位，用户和计算机帐户必须储存在单独的域中，也就是说，帐户域用于用户帐户，资源域用于计算机帐户。这是 Windows NT 标准，其中资源域通常以对单一帐户域(主域模型)或多个帐户域(多主域模型)的显式单向信任创建。

- 提供本地管理功能。

  在一个地理分散、设备分布的单位，通常期望授权本地人员管理资源。为允许在 Windows NT 系统中划分责任，建议以它们的自己的管理结构创建资源域。如同扩充 SAM 大小限制的情况一样，这会产生主域或多主域结构，而且这些结构具有对本单位帐户域的显式单向信任。这些信任的单向性质能保证资源域管理员只有对资源域的管理权限。

备注 作为升级规划的组成部分，管理模型必须反映升级资源域的所涉及的各方面问题。如果已经升级帐户域，然后将资源域升级为帐户域的子域，那么在它们之间会建立可传递信任关系。有鉴于此，必须考虑这种可传递信任如何影响资源的本地管理。

如果不希望管理权限扩展到资源域之外，必须考虑其它方案，这些方案包括：

将资源域重组到部门中

必须重新考虑域结构并考虑以后将资源域作为部门 (OU) 合并到升级的帐户域中。这种做法明显地影响对域升级顺序的考虑。

在现有的目录林内部升级资源域并使用 Windows 2000 管理功能委派

可以升级资源域使它与帐户域在同一目录林内，并使用 Windows 2000 管理功能委派以限制本地管理员的能力。在完成此步骤之前，检查资源域中的管理组并删除所有非该帐户域中的管理员。如果只有本地资源域管理员，添加一个或多个帐户域管理员。这些管理员能够在升级的同时管理域。作为进一步预防，要确保资源域管理员没有通过本地计算机帐户管理域控制器的权限。

在 PDC 升级之后，必须创建新的域本地组以保存资源管理员，并使用 Windows 2000 委派管理以赋予他们发挥作用的足够的特权。

将资源域升级为新目录林中的树

可以升级资源域并使其成为新目录林中的树，将此树通过显式单向信任链接到帐户域。这将有效地镜像在升级之前存在的结构。

确定升级域控制器的策略

域升级过程第一步是将 PDC 升级到 Windows 2000 Server。在升级 PDC 之后，下一个目标是尽快地升级域中的所有的 BDC。要将 Windows NT BDC 中不支持的 Windows 2000 功能的影响减到最少，此步骤是必要的。

Windows 2000 域模式

如果 PDC 没有升级到 Windows 2000，域仍是 Windows NT 域。在升级 PDC 和 BDC 的过程中，域处于中间运行状态，也称混合模式。可以让域无限期地运行于混合模式下或将它转移到最终的运行状态，也称“本机模式”。

混合模式

当以下几个条件之一存在，域就被认为是处于混合模式：

- PDC 已经升级但并非所有的 BDC 都已升级。
- PDC 和所有的 BDC 都已经升级，但还没有启用本机模式切换。

表 10.5 总结了混合模式下可用的 Windows 2000 功能，以及那些只有切换到本机模式才可使用的功能。如果不急于将域切换到本机模式，检查一下迁移目标，以确定维持在混合模式下是否危害您的目标，或各种利弊是否可以接受。

表 10.5 在混合模式下 Windows 2000 功能的可用性

功能	在混合模式下是否可用？
Kerberos 身份验证的可传递信任	是。Windows 2000 Server 和 Windows 2000 Professional 使用 Windows 2000 域控制器中具有的 Kerberos 服务。
Active Directory 部门 (OU)	是，但只有使用 Windows 2000 管理工具才可见。不能从 Windows NT BDC 或成员服务器管理。
Active Directory 安全组	否，只有全局和本地组可用。
IntelliMirror	是，但只对在 Active Directory 环境下运行 Windows 2000 Professional 的客户计算机可用。
Windows 安装服务	是。
64 位内存体系结构	是，具有硬件支持。
Active Directory 可扩展性	是，但只有当所有的 BDC 已经升级并正在运行 Active Directory 时可用。利用此功能必须谨慎，因为在域处于混合模式下仍可以添加新的 Windows NT BDC。此功能可能是回退规划的重要组成部分，因此决不能损坏。
Kerberos 身份验证	是，对于运行 Active Directory 的 Windows 2000 计算机。
Microsoft 管理控制台 (MMC)	是。
组策略	是，但只对在 Active Directory 环境下运行 Windows 2000 Professional 的客户计算机可用。
安全配置和分析	是。

Active Directory 多主复制	是，在 PDC 和已升级的 BDC 之间。

在决定将域切换到本机模式以前，域仍将处于混合模式，即使所有的 BDC 已经升级。

注意当您设置本机模式切换时，域仍可以包含运行 Windows NT Server 4.0 的成员服务器或运行 Windows NT Workstation 4.0 或 Windows 95 或 Windows 98 的客户机。

图 10.3 显示了从 Windows NT 域到本机模式 Windows 2000 域的过渡。

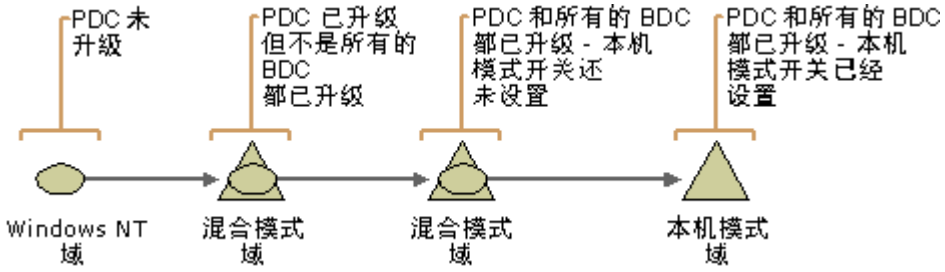


图 10.3 域升级模式

本机模式

“本机模式”是 Windows 2000 域的最终运行状态，可通过在用户界面设置开关启用。这就意味着升级的域现在被当作 Windows 2000 域，并且可以利用本章稍后的“切换到本机模式的理由”中所介绍的 Windows 2000 的全部功能。在将所有的域控制器升级到 Windows 2000 之后，便可以选择将域切换到本机模式。在切换时，发生以下几个事件：

- Netlogon 同步关闭，域在域控制器之间只使用 Active Directory 多主复制。
- 因为 Netlogon 同步被关闭，所以无法再将 Windows NT BDC 添加到域。
- 因为启用了多主复制，以前的 PDC 不再是域的主域，并且所有的域控制器可以执行目录更新。尽管如此，Windows 2000 仍将 PDC 模拟器角色指派到以前的 PDC。通常以前的 PDC 继续作为 PDC 模拟器，这在本机模式环境下意味着密码修改优先被其它域控制器复制到以前的 PDC。

  所有 Windows 2000 以前的客户机都使用 PDC 模拟器定位 PDC 并执行密码修改。另外，Windows NT 资源域也使用 PDC 位置信息建立信任。PDC 模拟器在本章稍后定义。

  组嵌套和 Windows 2000 组类型，如通用和域本地组都可用。

	重要决定 在决定将域切换到 Windows 2000 本机模式以前，它依然处于混合模式。可以让域无限期地在混合模式下运行，即使将域中所有的 BDC 都升级之后也是如此。然而，一旦将域切换到本机模式，它就无法返回到混合模式或变成 Windows NT 域。

升级 Windows NT PDC

当同步域中所有的 BDC，从而使他们完全用 PDC 中近期所做的改动更新了以后，就可以通过升级 PDC 来开始帐户域的升级了。当把核心操作系统安装到 PDC 以后，Windows 2000 安装程序检测到域控制器正在升级。安装程序然后提示您通过自动运行 Active Directory 安装向导把 Active Directory 安装到服务器上。

有关如何安装 Windows 2000 服务器的更多信息，请参阅本书中的“服务器自动安装与升级”。

Active Directory 安装向导为您提供下列选择：

- 在新目录林里创建第一个目录树
- 在已有的目录林中创建新目录树
- 为已有的域创建新的副本
- 安装子域

您的选择取决于您的名称空间的规划结果。 欲了解关于规划名称空间的更多信息，请参阅本书中的“设计 Active Directory 结构”，这是本章的前提。

在升级过程中，Windows NT 帐户数据库 (SAM) 的内容被复制到 Active Directory。这些对象是安全主管（用户帐户，本地和全局组，以及计算机帐户）。注意对于大帐户域来说，本过程会需要一些时间。

Active Directory 也包括对 Kerberos 身份验证的支持。在 Active Directory 安装向导完成后，Windows 2000 系统可使用 Kerberos 身份验证服务。这时，如果决定把含有已升级 PDC 的域加入已有的目录树，一个可传递的（双向）信任关系就和父域之间建立起来。任何在 PDC 升级之前创建的信任关系仍然存在，但他们是显式的单向信任。

Windows 2000 中的 PDC 仿真

由于 Active Directory 支持多主更新，一个 Windows 2000 域控制器和 Windows NT 4.0 的 PDC 不是同一种形式的 PDC。把 Windows NT 的 PDC 升级成 Windows 2000 域控制器后，它就作为 PDC，充当“PDC 仿真器”的角色。在 Windows 2000 里，每一个目录林中的域都有一个 PDC 仿真器。

PDC 仿真器通过如下方式支持 Windows NT 客户、成员服务器和域控制器，以及 Windows 95 和 Windows 98 客户：

- Windows NT、Windows 95 或 Windows 98 客户在 PDC 仿真器上进行目录写入（例如，密码更改）。
- 密码检查。
- Windows NT BDC 从 PDC 仿真器上复制。
- 在一个运行 Windows NT 浏览器服务的网络中，PDC 仿真器承担域主控浏览器的角色。它把 NetBIOS 名称注册为域名 <0X1B>。

在 Windows NT 客户、成员服务器和域控制器以及 Windows 95 和 Windows 98 客户全部升级以后，PDC 仿真器的这些功能就变得不必要了。

备注 Windows 2000 客户—和所有安装了 ADClient 程序包的 Windows 95 和 Windows 98 客户—可以用任何域中的域控制器来进行目录写入，如密码更改。这些活动不再局限于称为 PDC 的域控制器上。

PDC 仿真器在完全升级的 Windows 2000 的域中保留了某些功能。在域里由其他域控制器进行的密码更改将被优先复制到 PDC 仿真器上。当域中的一个身份验证请求由于另一个域控制器上的密码错误而失败时，域控制器在舍弃该请求之前，将身份验证请求转发给 PDC 仿真器。如果密码最近被更改过就这样做。帐户锁定在 PDC 模拟器上进行。当编辑服务器上的组策略对象时，组策略取默认值——PDC 模拟器。

有关安全策略的详细信息，参见 *Microsoft Windows 2000 Server Resource Kit Distributed Systems Guide*。

PDC 仿真器属性

在复制过程中，通过把 Active Directory 中的数据作为平直存储暴露给 Windows 95、Windows 98 和 Windows NT 的电脑（包括 BDC），PDC 仿真器可以提供向后兼容性。该兼容性通过如下方式得以说明：

- 对于其他 Windows 2000 的计算机，PDC 仿真器作为 Windows 2000 域控制器出现，对未升级的计算机则以 Windows NT PDC 出现。
- PDC 模拟器仍然可用来新建安全主管并把这些更改复制到 Windows NT BDC 上。
- Windows 95、Windows 98 和 Windows NT 客户可以用 PDC 模拟器作为一个可能的登录服务器。
- 如果 PDC 模拟器脱机或不可用，而域里有另一个 Windows 2000 域控制器，需要将那个域控制器作为 PDC 模拟器。如果域里不存在其他 Windows 2000 域控制器，那

么可以把 Windows NT BDC 提升为 PDC，然后再升级为 Windows 2000 服务器。

冲突解决

多主复制意味着，即使域控制器和网络其余部分断开，也可以在任何 Windows 2000 域控制器上执行更新。例如，如果您在一个断开的域控制器上执行更新，而同时其他人在另一个域控制器上执行与您的更新冲突的更新，那这两个更新在网络重新连接时都将复制。尽管存在更新冲突，所有域控制器将最终统一成相同数值。这个统一的过程称为“ 冲突解决 ”。

然而，有些冲突难以解决。假设不同的域控制器有互相冲突的目录架构版本。使用与 Active Directory 用来解决普通冲突时同样的原则可以解决架构冲突（“ 最后写入者决定 ”）。

访问控制组件

在 PDC 升级时，把安全主管移到 Active Directory 以后，一个主要问题是这个移动对资源访问的影响。以下部分说明了控制资源访问的组件。

安全标识符

Windows NT 的安全模型（Windows NT 和 Windows 2000 安全性的基础）可以通过安全标识符（SID）标识安全主管，如用户、组、计算机和域。SID 是域唯一值，在用户或组创建时建立，或者当计算机或信任在域中注册时建立。

SID 的组件遵循分级的约定。SID 包含标识修订号、SID 的颁发机构、域以及一些下级机构或相关标识符（RID）数值的部分，它们唯一标识与签发机构相关的安全主管。

重要 尽管有很多著名的 SID 可以跨越所有系统识别普通的组和用户，这里所说的安全主管还是要通过域的上下文来标识。这些安全主管不能在未更改 SID 的情况下在域之间移动。如果更改了 SID，资源访问将受到影响。然而，在升级时，安全主管保留在它们创建时所在的域中，因此标识安全主管的 SID 保持不变。这样，资源访问不受升级的影响。

身份验证和访问令牌

身份验证是 Windows NT 安全模型的一个基本组件。“ 身份验证 ”是一种方法，用户通过提供凭据（通常以用户名和密码的形式）被域识别。假设这些凭据是可以接受的，安全子系统为用户创建访问令牌，其中包括主 SID（用户的 SID）以及所有域和用户所在本地计算机组的 SID。每个用户创建的步骤，如应用程序的运行，都将带有用户访问令牌。

用户访问记号可以被看作一种呈现给系统的用户身份形式。系统用它来决定用户是否可以被授权访问系统资源。

授权和安全描述符

用户访问令牌的对应物是附加在资源（如文件和打印机）上的安全描述符并。安全描述符包含一个访问控制列表（ACL），它由访问控制项目（ACE）组成。一个 ACE 由一个 SID 和一个指示器组成，指示器指明由 SID 来标识的安全主管是被授予还是拒绝对某种资源访问权，如读取、写入和执行权限。系统通过把访问令牌中的 SID 和在 ACL 中的 SID 进行比较执行访问检查确认，从而来决定是否应该对申请的权限进行授权。

确定升级域的顺序

当您针对域控制器的升级有了一个即定的策略以后，下一步就是确定先对哪一个域进行升级。您的选择取决于您的整体升级目标。例如，如果您计划重组某些域，则不应该首先升级这些域。另外，如果一个已经存在的域将要成为目录林根，则必须首先将其升级。

建议按下列顺序升级您的域：

1. 帐户域
2. 资源域

升级帐户域的指导方针

一般说来，首先升级帐户域将使您收益最大，因为在许多情况下，需要管理的用户比计算机多。把帐户域升级到 Windows 2000 有如下好处：

- Active Directory 的可扩展性得到提高——许多组织正在用他们已有的用户和组的数量使推荐的 SAM 越来越大。Active Directory 提可高扩展性以便支持更大的运行各种各样应用程序的用户群。
- 委派管理——Windows 2000 的基础结构允许在很精细地委派管理职能，而不需要对本地的管理员授予绝对权利。

如果您有一个以上的帐户域，如下指导方针将帮助您选择一个升级的顺序：

减低风险并保持控制。即使您已经在实验室里或通过先导测试项目迁移测试了您的升级策略，第一个产品迁移仍然是最危险的。为了减低风险，先升级那些您最容易访问其域控制器的帐户域。

将损坏降到最低。首先，将那些用户较少的并且对域控制器有本地控制权的帐户域升级。这将在最大程度上降低对最多用户的破坏，尤其当您在部署过程中获得经验时。

完成作业。当您有了经验以后，对程序有了信心，而且已经降低了风险因素，就继续进行比较大的帐户域的升级，这很可能在日后成为对其他域的汇合点。随着用户基数的增长，Windows 2000 的功能将体现得更多。

识别作为重组目标的帐户域。如果您准备重组您的帐户域，先升级那些可能成为重建目标的域。您无法把域合并为不存在的目标域。标识那些将重组的帐户域。

升级资源域的指导方针

如果您有一个以上的资源域，用如下指导方针来确定升级的顺序：

选择那些其中的应用程序需要 Windows 2000 操作平台或功能的域。第一步，升级那些准备部署需要 Windows 2000 的基础结构或功能（如 Active Directory，它是 Microsoft Exchange 的下一个主要版本——Exchange Platinum 必须的）的应用程序的域。

选择那些有许多客户的域。下一步升级那些有很多 Windows NT 客户的域，以便您可以利用诸如 Microsoft® IntelliMirror™ 之类的 Windows 2000 的基础结构组件。

选择作为重组目标的域。对于帐户域，如果您准备重组资源域，首先升级那些可能成为重建目标的域。标识那些将重建的较小的资源域。

子域和信任

父域的域控制器最终把所有的架构和配置信息复制到新的子域中。在该信息被复制后，升级的域就成为 Windows 2000 目录树中功能完备的成员。注意该域将保持混合模式并且只能有限访问 Active Directory 的功能，直到您决定将其切换为本机模式为止。

Active Directory 认知客户，如运行 Windows 2000 Professional 或 Windows 95 或 Windows 98 （运行 Active Directory 客户软件）的计算机现在可以运用 Active Directory 并执行诸如查询全局编录（GC）来查找资源和人。可传递的信任允许存在于目录林的客户在该林范围内访问资源。这如何发生取决于客户是否在运行 Windows 2000 或 Windows 2000 以前的操作系统，如 Windows NT、Windows 95 或 Windows 98，也取决于目标域的升级状况。当客户存在于以下任何一个地方时，资源通过可传递的信任在目录林内可用：

- 本机模式域。
- 混合模式域，其中所有的域控制器已经被升级到 Windows 2000。
- 混合模式域，其中服务于 Kerberos 或 NTLM 身份验证申请的域控制器已经被升级到 Windows 2000。

在所有其他情况下，客户只能通过已经存在的单向显式信任访问资源，这些资源由于升级而保持不变。图 10.4 显示了可传递的信任如何运作于父域和子域之间。双向箭头表示域间可传递的信任。

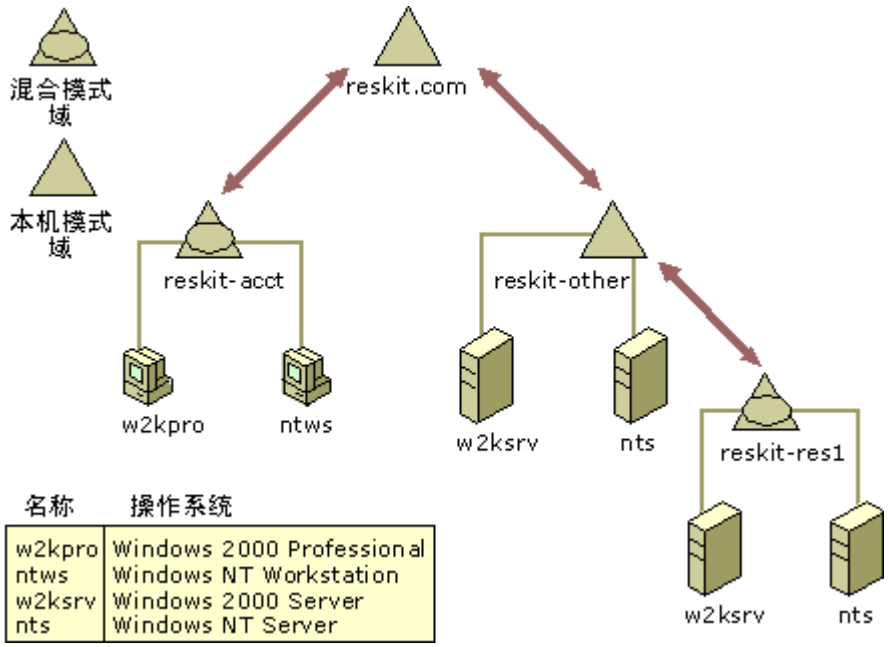


图 10.4 父域和子域间可传递信任示例

使用 NTLM 身份验证

NTLM 是一个身份验证协议，它是 Windows NT 网络身份验证的默认协议。为了与运行 Windows NT 版本的客户和服务器兼容，它保留在 Windows 2000 中

比如，一个用户从同一域的 Windows NT 工作站 *ntws* 登录到“reskit-acct.reskit.com”域，一个混合模式域，如图 10.5 所示。然后，用户试图与 “reskit-other.reskit.com”域（本机模式的 Windows 2000 域）中的 Windows NT 服务器建立网络连接。因为 NTWS 是一个 Windows 2000 以前的客户，它使用 NTLM。

Nts 确定在传递给它的凭据中指定的域名——“reskit-acct.reskit.com”，不是指它自己的数据库。所以 Nts 将登录请求发给在自己域内的域控制器进行身份验证。域控制器检查域名，由于它和域控制器的名称不符，域控制器检查它是否是一个信任域。域“reskit-acct.reskit.com”和“reskit-other.reskit.com ”的根同为“reskit.com”，因此这两个域之间有可传递信任。所以，域控制器把登录请求传递到信任域中的一个域控制器上。域控制器根据它自己的域帐户数据库，验证用户名称和密码，假设凭据相符，把帐户识别信息和组员身份表回传给和它联系的域控制器，然后后者再把它传给服务器。

服务器然后为用户创建一个模拟访问令牌，其中包含该用户的 SID 和该用户所在所有域组的 SID。处理客户请求的服务器使用一个线程模拟用户安全设置的上下文，它带有模拟令牌并试图代表用户访问资源。

这个例子表明，一个在混合模式中的 Windows 2000 以前的客户可以使用 NTLM 通过可传递信任访问一个在本机模式域中的 Windows 2000 以前的服务器。 由于同一目录林中所有的目录树都由可传递信任连接，所以即使两个域在不同的目录树时，也同样如此。

通过扩展，如果用户试图访问混合模式域“reskit-res1.reskit-other.reskit.com”中 Windows NT 服务器 nts 上的资源，只要从服务器收到登录请求的域控制器运行 Windows 2000，则该资源通过可传递信任在目录林中可以访问。

使用 Kerberos 身份验证

Kerberos 服务是运行 Windows 2000 的计算机的默认网络身份验证协议。在 Windows 2000 域内和 Windows 2000 域之间，安全套接字层 (SSL) 和 NTLM 身份验证，也可用于网络身份验证。Kerberos 身份验证是一个基于票据的协议，最初登录到域时，Windows 2000 域控制器上的密钥分发中心 (KDC) 发给用户票据授予票据 (TGT)。TGT 包含关于用户的身份验证信息而且通过一个叫 KDC 的密钥加密。当客户取得 TGT 后，它可以回传给域控制器，作为附加服务票据连接域中其它服务器的请求的一部分。当用户被授于一个 TGT 后，以后的检查将高效而迅速，因为域控制器只需要对 TGT 解密来检查用户凭据。服务票据与 TGT 类似，但是是用一个由服务器和域控制器共享的密钥加密的。

在图 10.4 所显示的例子中，用户现在象以前一样登录到域“reskit-acct.reskit.com”，但这次是从同一个域中的计算机“w2kpro ”上，该机运行 Windows 2000。用户想与在域“reskit-other.reskit.com ”中的 Windows 2000 服务器：“w2ksrv ”建立连接。因为“w2kpro ”是 Windows 2000 的客户，客户试图使用 Kerberos 协议。

Kerberos 协议与 NTLM 一样，可跨越域边界运行。如果两个域之间已经建立了信任关系，一个域中的客户可以通过身份验证登录到另一个域中的服务器上。当域间建立了信任，它们可以交换域间密钥。每个域的身份验证服务使用自己的域间密钥对到另一个域的 KDC 的票据加密。

当客户想访问远程域中的服务器时，该客户联系本地域上的域控制器取得一个 TGT。如果客户与远程域或它的父域之间有直接信任关系的话，则该客户可把 TGT 传给远程域上域控制器的 KDC。对于所有中级域，这一过程不断重复，直到在客户的本地域和远程域之间建立了信任路径。

客户把推荐的 TGT 传给远程域控制器的 KDC，申请一个到客户域中服务器的票据。远程域控制器使用它的域间密钥对客户的 TGT 解密。如解密成功，则远程域控制器可确认该 TGT 是由信任机构发出的。远程域控制器然后授予该客户一个到申请的服务器的票据。

图 10.4 显示了一个信任路径可以在两个域，即“ reskit-acct.reskit.com ” 和“ reskit-other.reskit.com ”之间建立，因为它们是同一个根的子域而且它们之间有可传递信任。收到推举 TGT 后，目标域中的域控制器检查它是否有该服务器的共享密钥。如果有，域控制器给客户颁发一个服务票据。因为 “ w2ksrv ”是 Windows 2000 计算机，而且有一个共享的密钥，所以可以给“ w2kpro ”颁发一个票据。

本例子的关键因素是在运行 Kerberos KDC 的目标域中存在一个域控制器，而且在域控制器和服务器之间有一个共享的密钥。Windows 2000 的域控制器有作为 Active Directory 安装过程一部分被启用的 Kerberos 服务，另外，增加一个 Windows 2000 域的成员服务器涉及创建一个共享密钥。由此，只要有 Windows 2000 域服务器颁发会话票据，“ w2kpro ”就可以使用 Kerberos 访问“ w2ksrv.reski-res1.reskit-other.reskit.com ”。

如果“ w2kpro ”试图访问 Windows NT 计算机上的资源，比如“ nts.reskit-res1.reskit-other.reskit.com ”，Kerberos 身份验证失败，客户然后试图进行 NTLM 身份验证，如本节早些时候在“ 使用 NTLM 身份验证 ”中所描述那样。

确定切换到本机模式的时间

把域从混合模式切换到本机模式很容易，但该切换无法撤消。为了确定何时进行切换，您需要考虑本节的所有因素。如果该域目前包含或将要包含任何 Windows NT 域控制器，则无法把域切换为本机模式。

继续在混合模式的理由

继续使您的域处于混合模式的主要原因如下：

无法升级应用程序服务器

您有无法升级或降级为成员服务器的应用程序服务器。
比如，为获取高吞吐量，某些应用程序需要安装到 BDC 上，以避免通行身份验证。
存放这样的应用程序的 BDC 称为“ 应用程序服务器 ”。

BDC 的物理安全性不足

在域的规划中，安全性是一个重要考虑因素。安全性的一个基本方面是计算机本身的物理安全性；实际上任何容易访问的计算机都易受攻击。这里的一个考虑因素是，只通过 PDC 的 SAM 单主更新与通过所有域控制器的帐户数据库 Active Directory 多主更新之间存在差别。

由于 Windows NT 目录更新的单主特性，您可能对 BDC 上的相对轻松的安全性感到舒服。如果是这样，把它们升级为 Windows 2000 域控制器时需要重新考虑这一点。如果您无法适当地升级 BDC 的安全性，您可以考虑在升级时，把 BDC 降级为成员服务器，在一个不同的位置增加一个新的 Windows 2000 域控制器，或是可以重新考虑您建议的域结构。

完全回退到 Windows NT 仍然必要

混合模式的好处之一是向后兼容程度。如果出现问题，混合模式允许把新的 BDC 填加到域中。在新的 BDC 加入域中以后，您可以进行帐户数据库的再同步。只要没有其它 Windows 2000 域，您就可以将 BDC 提升为 PDC。

您要为回退和故障恢复作准备，但是有时您会想完全切换到新环境中以便充分利用 Windows 2000 的功能。

一个很好的原因是切换到本机模式使您可以使用所有的 Windows 2000 组，包括套装的组。在这时，需要考虑您可能想把哪些组升级为通用组。

切换到本机模式的理由

尽管把您的 PDC 和 BDC 升级并把域保持在混合模式时获得很大好处，您最好还是尽快切换到本机模式。本机模式可以帮您在以下方面提高您的网络的整体功能：

- 新的 Windows 2000 组类型可用。
- 本机模式域可以使用通用组和组嵌套。

正如所讨论的那样，切换到本机模式是不会自动进行的；您必须通过 Microsoft 管理控制台 (MMC) 的 Active Directory Domains and Trusts 管理单元进行更改。关于如何使用这个管理单元的详细信息，请看 Windows 2000 Server 帮助文件。

检查 Windows 2000 组

确定迁移到 Windows 2000 将对安全策略和 Windows 2000 以前的结构有如何影响是很重要的。对安全策略的改变将很可能要求重组组。

Windows 2000 支持四种类型的安全组：

- 本地
- 域本地
- 全局

- 通用

本地组

“本地组”存在于 Windows NT 中，可以包含目录林中、在其它受信任的目录林中、或在受信任的 Windows 2000 以前的域中任意位置的成员。然而，本地组只可给它们存在的计算机赋予资源访问权限。

Windows NT 中本地组的特殊情况是那些在 PDC 中创建的本地组。在 BDC 之中复制域 SAM 产生在 PDC 和 BDC 之间共享的本地组。在混合模式下，本地组在 Windows NT 和 Windows 2000 中作用相同。在本机模式下，域控制器中的本地组变成域本地组，这在下一小节介绍。通常，本地组用于赋予访问本地计算机的资源的具体权限。

域本地组

“域本地组”是 Windows 2000 的新功能，尽管在概念上和用法上与在 Windows NT 域中创建的本地组相似。

域本地组只能在本机模式域中可用，并可包含目录林中、在受信任的目录林中、或在受信任的 Windows 2000 以前的域中任意位置的成员。本地域组只能授予对它们所在的域中的资源的权限。通常，本地域组用于从域林收集安全负责者来控制对域内资源的访问。

全局组

Windows 2000 全局组实际上与 Windows NT 全局组相同。Windows 2000 全局组只可包含它们所在的域内部的成员。可以给这些组赋予访问目录林中或受信任的目录林任何域的资源的权限。

通用组

“通用组”可以包含目录林中的任何 Windows 2000 域的成员，并可以赋予访问目录林中的或受信任的目录林中的任何域的权限。尽管通用组可以有相同目录林中的混合模式域的成员，此类域的成员没有通用组加到它们的访问令牌，因为通用组在混合模式下不可用。尽管可以将用户添加到通用组，但建议限制全局组的成员身份。注意通用组只能在本机模式域下可用。

可以使用通用组建立执行企业内部常见工作的组。举一个例子，如虚拟组。一家大公司的此类组的成员可以是全国性的、或世界性的，当然也可以是全目录林的，组资源分布类似。在这些情况下，通用组可用作保存每个分支机构或部门的全局组的容器，组资源通过通用组的单个 ACE 保护。

通用组和它们的成员列在全局编录 (GC) 中。尽管全局和域本地组也列在 GC 中，但它们的成员并没有。这与 GC 复制通讯量有关。建议小心使用通用组。如果您的整个网络有高速连接，可以直接对所有的组使用通用组，并具有不必管理全局组和域本地组的优点。然而，如果您的网络跨越广域网 (WAN)，可以使用全局组和域本地组改进性能。

如果使用全局组和域本地组，还可以将任何广泛使用的很少改变的组指派为通用组。

表 10.6 列出了 Windows 2000 组的属性。

表 10.6　Windows 2000 组属性

组类型	成员来自	作用域	在混合模式下是否可用？
本地	相同的目录林 其它受信任的目录林 受信任的 Windows 2000 以前的域	全计算机	是
域本地	相同的目录林 其它受信任的目录林 受信任的 Windows 2000 以前的域	本地域	否
全局	本地域	任何受信任域	是
通用	相同的目录林	任何受信任本机模式域	否

嵌套组

建议将组大小限制在 5,000 个成员，因为 Active Directory 存储器必须能够一次更新。因为组成员储存在单个多值属性中，对成员的修改要求整个成员列表在域控制器之间复制并在单个事务内更新。Microsoft 测试了并支持多达 5,000 个成员的组成员身份。

然而，可以将组嵌套以增加成员的有效数量。这么做将有助于减少由组成员修改的复制引起的通讯量。嵌套方案取决于域是在本机模式下还是在混合模式下。下列列表介绍在本机模式域存在的组可以包含什么。这些规则由组的作用域决定。

- 通用组可以包含任何域的用户帐户、计算机帐户、通用组和全局组。
- 全局组可以包含来自相同域的用户帐户和计算机帐户，和来自相同域的全局组。
- 域本地组可以包含来自任何域的用户帐户、计算机帐户、通用组，和全局组。它们还可以包含来自相同域内部的其他域本地组。

混合模式域中的安全组只可以包含：

- 可以包含来自受信任域的全局组和用户帐户的本地组。
- 只包含用户帐户的全局组。

组成员身份扩展

当用户登录到客户机或与服务器进行网络连接时，用户的组成员扩展为建立用户访问令牌的组成部分。组扩展的发生过程如下：

在交互登录到客户机时，客户机联络域控制器以校验用户凭据并获得 Kerberos TGT。域控制器扩展以下几个组类型的用户的所有的组成员列表：

- 在目录林中任意位置定义的通用组
- 全局组
- 与用户帐户相同的域的域本地组。

这些组列表作为授权数据包括在 TGT 中。

- 当客户机启动与服务器的网络连接时，如果服务器位于与用户帐户不同的域，将使用跨域引用以从服务器的 KDC 取得服务票据。当发给服务票据时，组扩展将添加域本地组，其用户是服务器的域的成员。这些组与 TGT 中的组列表一起加到服务票据的授权数据中。如果服务器位于与用户帐户相同的域，域本地组从最初的交互登录时就已经可用。
- 当客户机连接到服务器时，如果用户帐户、或其用户是成员的组之一也是服务器中任何本地组的成员，那么本地组的扩展发生。

当创建用户访问令牌时，由域控制器或资源服务器扩展的所有的组成员信息都用于标识用户。

升级对组的影响

将 PDC 升级到 Windows 2000 对组没有直接影响：Windows NT 本地组变成 Windows 2000 本地组，而 Windows NT 全局组变成 Windows 2000 全局组。当您将域切换到本机模式时，发生实际的改变，此时 PDC 中的本地组变成域本地组。

在 Windows 2000 中使用 NetBIOS

NetBIOS 是高级网络编程接口，它用于 Windows 2000 以前的网络组件中。网络资源在 NetBIOS 名称空间中由唯一 NetBIOS 名称标识。WINS 是作为 Windows NT Server 4.0 的组成部分提供的一种服务，它支持 NetBIOS 名称动态映射到 IP 地址的注册，并提供 NetBIOS 名称解析。

发布 Windows 2000 后，对 NetBIOS 命名接口的支持只在群集服务器上需要。有鉴于此，随着 DNS 的使用和 Active Directory 的出现，NetBIOS 的使用将随着时间的推移日渐淡化。

注意将域升级到 Windows 2000 不一定消除网络中对 NetBIOS 支持的需要，也不影响当前的支持程度。例如，如果网络是多段的，则要求 WINS 以创建 NetBIOS 浏览列表。没有 WINS 网络必须依赖 Active Directory 浏览资源。这会对 Windows 以前的客户机有很大影响。

如果符合以下几个条件，则可以在升级之后停止 NetBIOS 的使用：

- 没有客户机（如 Windows for Workgroups、Windows 95、Windows 98 或 Windows NT）和没有运行使用 NetBIOS 的 Windows NT 的服务器。然而，运行 Windows 操作系统早期版本的客户机可能仍要求 NetBIOS 名称以提供文件和打印服务并作为对传统应用程序的支持。

  在测试规划中，要确保评估传统应用程序和服务的影响。有关测试的详细信息，参见本书的“ 建立 Windows 2000 测试实验室 ”。

- 网络是纯 Windows 2000 网络并确信网络中的所有的计算机和应用程序使用另一个命名服务（如 DNS）能正常工作。网络命名是在网络中定位计算机和资源的重要服务，甚至不需要 NetBIOS 名称的地方也是如此。

  Windows 2000 WINS 客户机本地缓存解析的名称并使用名为 Caching Resolver 的组件在将查询提交到 DNS 之前搜索缓存。客户机开始运行时就开始缓存 HOST 文件，并且对 HOST 文件的任何更新都立即反映在缓存中。名称解析顺序如下：

  1. 客户机从客户机缓存中尝试名称解析。
  2. 如果从客户机缓存解析失败，客户机通过 DNS 尝试名称解析。
  3. 如果 DNS 名称解析失败，客户机尝试通过 WINS 解析。

如果符合这些标准，从 NETBIOS 和 WINS 移走是无缝的，只要您在最近升级的客户机上实现足够的修改控制即可。

过渡到文件复制服务

Windows NT Server 提供一种也称为 LAN 管理器复制服务的复制功能。在 Windows 2000 Server 中文件复制服务 (FRS) 代替了 LAN 管理器复制服务。

备注 Windows 2000 Server 在混合或本机模式下不支持 LAN 管理器复制服务，因此如果您使用了 LAN 管理器复制，必须在升级规划中包括一种策略移到 FRS 以提供相同的功能。

LAN 管理器复制服务过程

LAN 管理器复制服务使用导入和导出目录的概念。选择在上面存放导出目录的服务器和存放导入目录的许多服务器，配置 LAN 管理器复制服务。存放目录的服务器不一定是域控制器，它们可以是普通成员服务器。图 10.5 是 LAN 管理器复制服务过程。

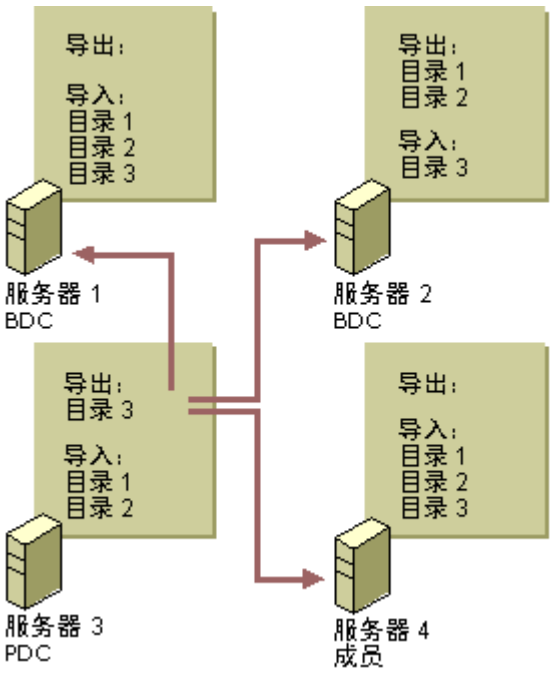


图 10.5 LAN 管理器复制服务过程

FRS 过程

FRS 在 Windows 2000 Server 中自动配置以使每个域控制器有复制的系统卷 (SYSVOL)。对储存在任何域控制器的 SYSVOL 中的登录脚本所做的任何修改都以多主形式复制到其他域控制器中。与 LAN 管理器复制不同,在 LAN 管理器复制中普通成员服务器可以存放导入和导出目录,而 FRS 只有域控制器才可以存放 SYSVOL。图 10.6 是 FRS 过程。

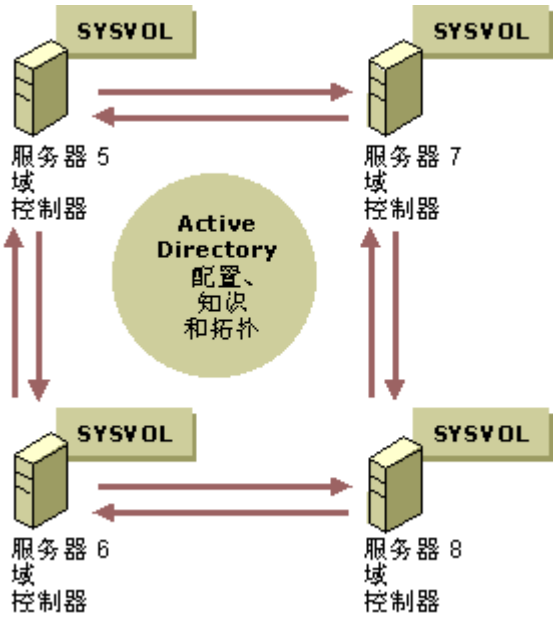


图 10.6 FRS 过程

在混合环境下维护 LAN 管理器复制服务

在升级时，可以维护 Windows NT BDC 和运行 Windows 2000 域控制器的成员服务器的混合环境。因为 Windows 2000 Server 不支持 LAN 管理器复制服务，混合环境的维护是一个问题。为提供这种支持，必须在 LAN 管理器复制服务和 FRS 之间建立网桥以使这两种服务都可以运转。这可通过选择 Windows 2000 域控制器，将文件复制到 Windows NT 导出目录完成。复制通过定期安排的名为 L- bridge.cmd 的脚本完成。

备注 不要将“ 混合环境 ”与“ 混合模式 ”这两个术语搞混，后者是指 Windows 2000 域内 PDC 和零或更多 BDC。“ 混合环境 ”是指在混合或本机模式下 Windows 2000 域并包含 Windows 2000 以前的客户机或服务器。

在 LAN 管理器复制服务和 FRS 之间安装网桥

在 LAN 管理器复制服务和 FRS 之间安装网桥之前，必须执行下列步骤：

- 确定目录的 Windows NT 导出服务器。
- 选择可以将文件推到该目录的 Windows 2000 计算机。

建议手动在每个域控制器或成员服务器升级之前从“ 控制面板 ”中“ 服务 ”中的“ LAN 管理器复制服务 ”停用。尽管不推荐，可以在升级之后从 MMC 停用目录复制程序。

若要在升级到 Windows 2000 之前升级导出服务器，执行以下几个步骤：

1. 在当前导出服务器上运行 SrvMgr.exe 并删除导出目录。
2. 从新的导出服务器上，通过 SrvMgr.exe 将导出目录添加到导出列表。

一个批处理文件提供 Windows NT 脚本目录和 Windows 2000 系统卷之间的链接。这种方法的优点是两种复制机理在物理上彼此分开，因此传统服务可引入到 Windows 2000 域控制器。

要为 LAN 管理器复制服务和 FRS 的网桥安装批处理文件，执行以下几个步骤：

1. 选择 Windows 2000 域控制器。
2. 创建名为 L- bridge.cmd 的批处理文件，将登录脚本复制到 Windows NT 导出服务器，如下面的举例所示。

   ```
   xcopy \\domain.com\Sysvol\domain.com\scripts \\Srv3\Export\scripts /s /D
   ```

   注意 /D 命令行开关告诉 xcopy 只复制较新的文件。/s 命令行开关告诉 xcopy 复制目录和所有的子目录（倘若它们不是空的）。

3. 使用 Windows 2000 计划任务服务，设置待运行的批处理文件的合理的时间间隔。每隔两小时的时间间隔绰绰有余，特别是因为使用 /D 选项防止创建不必要的文件副本。

L- bridge.cmd 的示例版本在 Windows 2000 Resource Kit CD 中可以找到。

使 LAN 管理器复制服务在升级时可用

要使 LAN 管理器复制服务在升级时可用，必须只有在所有的存放导入目录其它服务器升级之后升级存放导出目录的服务器。如果存放导出目录的服务器是 PDC，必须选择新导出服务器并重新配置 LAN 管理器复制服务。建议您选择的新服务器是您相信将是最后一个待升级到 Windows 2000 的服务器，否则，必须选择另一个导出服务器并再仔细检查一遍过程，因为服务器是按顺序升级的。

在混合环境下使用路由和远程访问服务

如果在 Windows NT 环境下使用路由和远程访问服务 (RRAS) 以提供用户到企业网络的远程访问，在升级成员服务器的过程中尽早考虑升级 RRAS 服务器。因为 RRAS 进程在 Windows NT 中的工作方式，特别是，它检查 RRAS 属性如 RRAS 访问的可用性或用户的拨回的方式，尽早升级很重要。

即使没有用户登录到系统，RRAS 也必须运行。服务作为 LocalSystem 运行。当服务登录为 LocalSystem 时，它以 NULL 凭据登录，这意味着服务不提供用户名或密码。这意味着帐户不能用于依赖 NTLM 身份验证访问网络资源，除非远程计算机允许以 NULL 凭据访问（称为 NULL 会话）。Windows NT 中的 RRAS 使用 LocalSystem 帐户。

默认时，Active Directory 不接受通过 NULL 会话的对象属性查询，因此在混合环境中，Windows NT RRAS 服务器不能检索用户 RRAS 属性，除非符合下列所有的条件：

- 域处于混合模式下并且 Windows NT RRAS 服务器也是 BDC。在这种情况下，RRAS 可以本地访问 SAM。
- 域处于混合模式下并且 Windows NT RRAS 服务器联系 Windows NT BDC，这会产生与当前 Windows NT 作用相同的作用。这种作用是基于安全通道的位置进行的。
- 域处于混合或本机模式并且 Active Directory 安全放松赋予“每个”内部用户权限以阅读任何用户对象中的任何属性。Active Directory 安装向导允许用户通过某些 Active Directory 对象中的“减弱权限”选项选择这种配置。

只有在理解了其对 Active Directory 安全的影响之后才能使用最后一个条件中的解决办法。如果这种解决办法与安全要求相抵触，建议将 Windows NT RRAS 服务器升级到 Windows 2000 并使其成为 Windows 2000 混合或本机域的成员。这将防止在域处于混合模式下时的不一致的、如第二个条件中所介绍的作用。

规划域重组

域升级允许您维护尽可能多的当前环境，包括域结构，而域重组允许您根据本单位的需要重新设计目录林。尽管域重组可以有各种不同的结果，通常当前结构被改组为较少的、更大的域。

Windows 2000 提供本机功能以允许按如下方式进行域重组：

- 安全主管可以从一个域移到另一个域，同时在移动之前维护到可用的资源的访问。

- 域控制器可以从一个域移到另一个域，而不必完成操作系统的重新安装。

备注　域重组不是部署 Windows 2000 Server 的要求。可以在需要时随时重组。将计算机移到新域并更新或校验访问控制是一项工作量大且费时的工作。

为帮助进行域迁移，Microsoft 开发了“域迁移基本工具”（*Domain Migration Basic Utilities*）。这些工具包括组件对象模型（COM）对象和设计作为适合用户的管理工具的基础的脚本示例，以及支持许多 Microsoft 编写和测试的域迁移示例。这些示例是基于用户的有关它们的迁移要求的反馈信息而开发的。基本工具 ClonePrincipal 在本章稍后介绍。

确定重组域的理由

本章的重点是从 Windows NT 到 Windows 2000 的最初迁移。本章稍后所介绍的一些重组方法可能在迁移后阶段有用。

尽管您可能有许多重组域的理由，但主要理由是充分利用 Windows 2000 的功能。通过这些功能，可更好地利用域反映本单位的要求。重组域的一些主要优点包括：

可扩展性更强。您可能围绕 SAM 帐户数据库的大小限制设计了以前的 Windows NT 域结构，能引导您实现主域或多主域模型。由于 Active Directory 的可扩展性大大地增强，能扩展到数百万用户帐户或组，可以将当前 Windows NT 域重组进较少的、更大的 Windows 2000 域。

委派管理。在当前模型中您可能实现资源域以允许委派管理责任。Windows 2000 OU 可以包含任何类型的安全主管，并且管理可以按您的要求委派。在许多情况下，将资源域转换为 OU 更适合委派管理。

管理更加细化。为使管理责任更加细化，也许由于企业并购，域结构可以通过复杂的信任网连接。您可能想将一些域实现为 OU 以简化管理，或重新设计域模型以利用较少的显式信任的优点。

注意下一小节介绍的示例不要求完成升级，尽管一些重组方法可能要求将计划重组的域中的 BDC 首先升级。

确定重组域的时间

视迁移规划的情况，可以选择在升级之后立即重组域，代替升级，或将来某些时候作为常规域重新设计。这些方案介绍如下：

升级后

域重组的最可能的时间是在升级之后，作为迁移到 Windows 2000 的第二阶段。升级已经解决了不太复杂的迁移问题，如域的组，在其中信任结构基本上正确并且没有管理问题。

当选择在升级之后重组时，您的目标最可能包括重建域结构以降低复杂性，或以安全的方法将权限低的管理员的资源域带进目录林。

代替升级

您可能觉得当前域结构不能恢复(例如，如果必须重新设计目录服务基础结构以利用 Active Directory），或在迁移时不能危害当前生产环境的稳定。不论发生哪种情况，最容易的迁移途径可能是设计并建立“ 原来的目录林 ”：一种与当前生产环境分开的理想的 Windows 2000 目录林。这能确保在先导测试项目运行期间工作能正常进行，并且先导测试项目最终会变成生产环境。

在建立先导测试项目之后，可以将少数用户、组、和资源迁移进先导测试中开始域重组。当本阶段成功完成之后，将先导测试项目过渡到向新环境分阶段的迁移。随后，建立 Windows 2000 生产环境，淘汰旧的域结构，并重新部署其余的资源。

迁移后

在这一阶段，作为纯粹 Windows 2000 环境常规域重新设计的组成部分，开始进行域重组。这可能要一直进行好几年，如发生机构变动或企业并购时，当前结构就变得不合适了。

检查重组域的相关问题

在确定必须重组域的原因和时间之后，必须检查此类重组的相关事项。下面几节介绍：

- 移动安全主管、用户和全局组、计算机、和成员服务器。
- 建立信任。
- 复制安全主管。

移动安全主管

使域重组从根本上得以实现的是在 Windows 2000 的域之间移动安全主管和域控制器。这有许多重要相关问题，如，系统如何识别安全主管，如何维护对资源的访问。此类相关问题会影响域重组的首选方法。

对 SID 的影响

SID 与域相关的性质具有下列后果：当您在域之间移动用户或组之类的安全主管时，必须给安全主管颁发一个新域的帐户的新 SID。

在 Windows NT 安全模型中，对资源的访问以如下方式受影响：操作系统查看用户访问令牌并将用户的主 SID — 以及用户所在任何组的 SID — 与资源安全描述符中的 ACL 进行比较。因为 SID 的列表在 ACL 中包含会引起对 SID 识别的安全主管的访问被允许或拒绝的信息，改变 SID 有长远的影响。

改变 SID 的相关问题在下列举例和图 10.7 中图解。Bob 是 Reskit Corporation 的员工并在 Windows NT 帐户域 Reskit-Acct 中有一帐户。Bob 也是相同域的全局组“ Finance Analysts ”的成员。

Reskit Corporation 使用运行于资源域 Reskit- Res1 中的许多 Windows NT 服务器的 Windows NT 财务应用程序。因为在 PDC 中创建的本地组在域中所有的域控制器之间共享，运行应用程序的服务器也设置为域的 BDC。共享本地组“ Financial Resources ”在 PDC 上创建并用于应用程

序使用的文件的 ACL 中。全局组“ Reskit- Acct\Finance Analysts ”是“ Reskit- Res1\Financial Resources ”的成员。

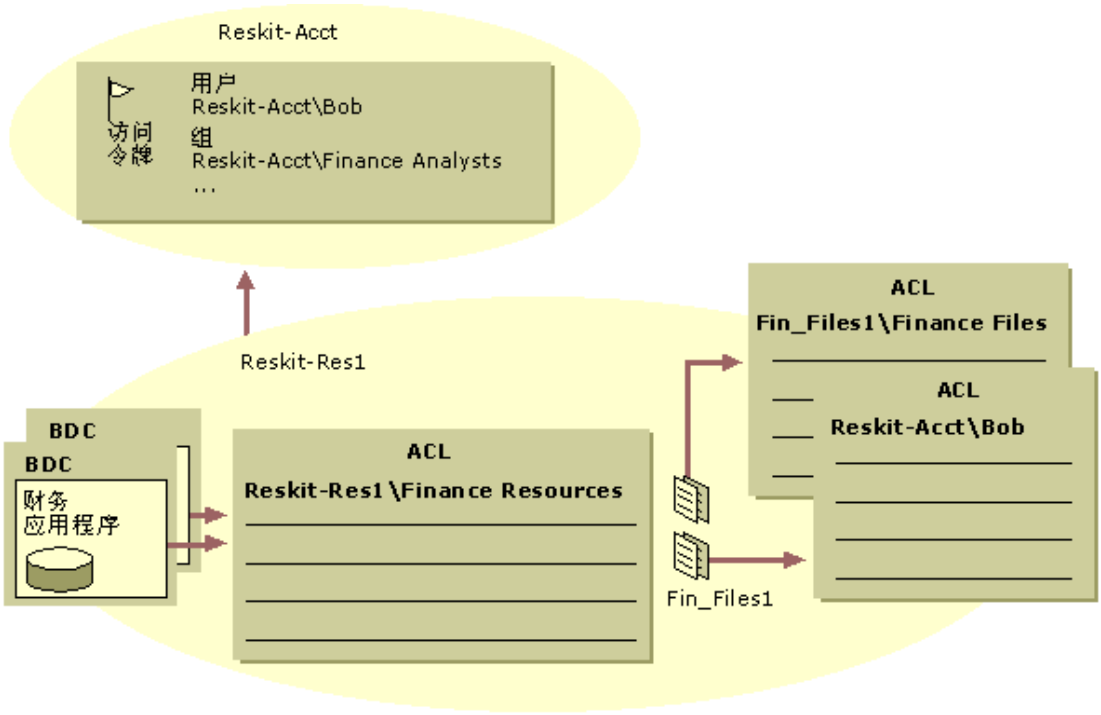


图 10.7 资源访问举例

Bob 也有文件服务器（资源域中的 Fin_Files1）的访问权。Fin_Files1 是设置为成员服务器的 Windows NT Server。Fin_Files1 使用与 Reskit- Acct\Finance Analysts 有关的文件的 ACL 本地组“ Finance Files ”，Reskit- Acct\Finance Analysts 是 Fin_Files1\Finance 文件的成员。Bob 在一些私人项目工作，在受保护的 Fin_Files1 上有一个目录，只有他可以访问该目录中的文件。此目录有一包含单个项的 ACL，允许 Bob 对目录完全控制。

移动安全主管的相关问题可以通过跟踪 Reskit- Acct\Bob 移到另一个域作为与域重建有关的迁移的组成部分时会发生什么情况看到。在本例中，Reskit- Acct 已经升级到 Windows 2000，将 Windows 2000 目录林作为根域 reskit.com 的子域加入。域 Reskit- Acct 已经被切换到本机模式，但也被重建，且其成员移到目录林的另一部分的名为 Reskit- Acct2 的 Windows 2000 域。

备注 本例阐明了当通常所说的“ SIDhistory”这一 Windows 2000 功能不可用时会发生什么情况。弄清如果在重组时出现这种情况如何处理是很重要的。注意 SIDhistory 在本章稍后讨论。

对全局组成员身份的影响

Reskit- Acct\Bob 是全局组 Reskit- Acct\Finance Analysts 的成员。因为全局组只可包含其自己域的成员，将 Bob 移到新域将引起他的新帐户从 Reskit- Acct\Finance Analysts 排除。Bob 将失去对 Reskit- Acct\Finance Analysts 可用的有价值的资源的访问权限。

假设在新域和资源域之间存在足够的信任，这种情形似乎可以多种方法解决。

将新的 SID 添加到资源 ACL

对资源的访问可以通过将 Bob 的新 SID 添加到他以前作为 Reskit- Acct\Finance Analysts 的成员时有访问权的所有的资源中的 ACL 中。这种解决办法由于下列原因而费时又复杂：

- 许多域重组工作在一段时间内逐步实现的。没有保证在那段时间内新资源不会为 Reskit- Acct\Finance Analysts 创建。因此，“ 重新许可 ”将不得不在重组时间内继续。

- 如果 Bob 将更换工作，不再需要是 Reskit- Acct\Finance Analysts 的成员，从 Reskit- Acct\Finance Analysts 删除 Bob 比改变引用他的资源的 ACL 更为容易。建议使用组而不用个别的人设置 ACL，因为用户和他们的具体工作可以随时改变。

移动组

因为安全主管可以在 Windows 2000 内移动，Reskit- Acct\Finance Analysts 可以移到新域。然而，引用组的 ACL 也引用组 SID，因此必须重新许可资源以引用新 SID。

在目标域中创建“ 平行 ”组

如果 Reskit- Acct\Finance Analysts 移到另一域，如果所有的组成员不一次移动，会发生一个问题。这意味着组必须在旧的域内维护，新的“ 平行 ”组在新域中创建。资源访问将为原始的组及其成员维护，但必须重新分配资源许可以赋予访问新组的权限。再者，重新许可必须在组同时存在于两个域时继续。

注意这就是当 SIDhistory 不可用时发生的情况。SIDhistory 在本章稍后讲述。

对直接引用用户的 ACL 的影响

也允许 Reskit - Acct\Bob 直接访问成员服务器 Fin_Files 中的一些资源，因为他的 SID 出现在那个服务器上的 ACL 上。将用户添加到资源上的 ACL 中是完全合法的，但移动 Reskit - Acct\Bob 将要求那个服务器上的资源重新许可。这就将新域 SID 添加到 Bob 的帐户。

SIDhistory

在许多情况下，Reskit Corporation 举例中的活动由于 Windows 2000 的 SIDhistory 功能变得不必要。SIDhistory 是 Active Directory 安全主管的属性，用于储存移动物体（如用户和安全组）以前的 SID。

当使用 Microsoft 提供的 Windows 2000 工具移动用户时，Active Directory 中的用户对象的 SIDhistory 属性随以前的 SID 更新。当用户登录到系统，系统检索用户 SIDhistory 中的项目并将它们添加到用户访问令牌。因为组可以移动，系统也检索用户是其成员的所有的组的 SIDhistory 属性并将这些属性添加到用户访问令牌。

令牌中的 SIDhistory 项目在授权检查时对系统来说象正常的组成员，并且在对 Windows 2000 或 Active Directory 毫不知情的 Windows 2000 以前的系统中允许适当的访问。图 10.8 是如何使用 SIDhistory 允许资源访问的图解。

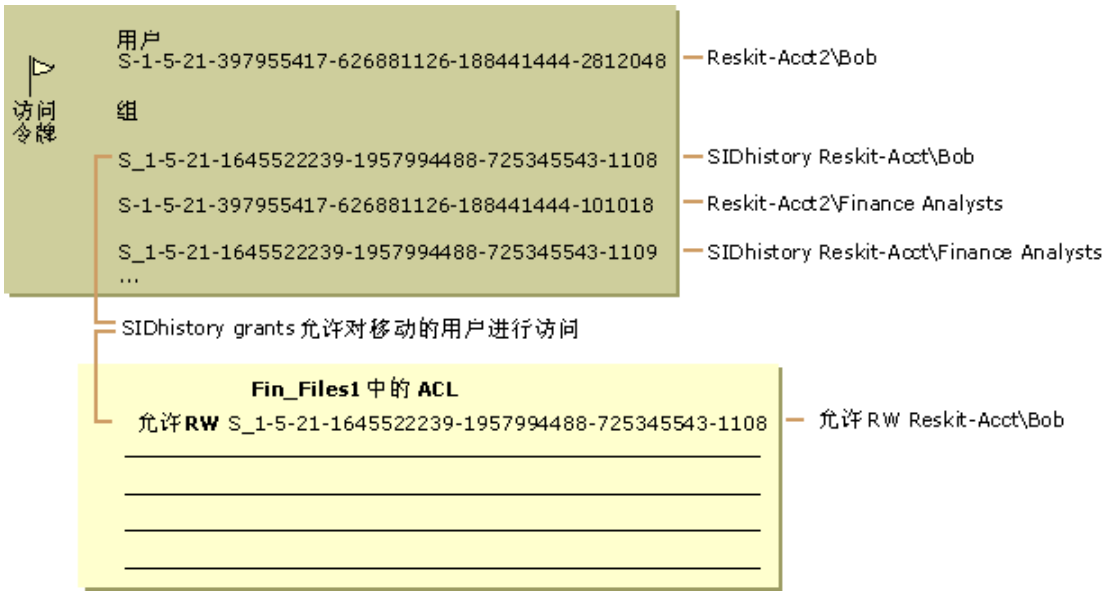


图 10.8 通过 SIDhistory 允许的资源访问

Windows NT 3.51 和 SIDhistory

关于组成员身份和在 Windows 2000 域中使用 Windows NT 3.51 有一个问题。该问题涉及 Windows NT 3.51 从域控制器接收组成员身份 SID 和建立安全访问令牌的方式。当对用户进行身份验证时，Windows NT 3.51 访问令牌只使用相对于用户帐户域和进行身份验证的服务器或客户机的本地组的 SID 建立。结果，Windows NT 3.51 系统不能识别来自外部帐户域的通用组，或来自资源域的域本地组。

因为用户的 SIDhistory 中的项目或用户所在的任何通用组的项目都来自不同于帐户域的域，这些项目都从令牌中排除。问题是对于 Windows NT 3.51，来自不同于登录用户的帐户域的域的组成员 SID 在评估访问控制时被忽略。在大多数情况下，访问被拒绝，尽管这可能不是想要的结果。

移动用户和全局组

因为全局组只可包含其自己的域的成员，当用户在域之间移动时，用户是其成员的任何全局组也都必须移动。必须这样才能维护对受引用全局组的 ACL 保护的资源进行访问。这种情况的必然结果是如果全局组移动，其成员也必须移动。

在此情况下，一个封闭的用户和全局组的集合是这样一个集合，在其中下列论述为真：

- 对于每个移动的用户，该集合中的所有的全局组也是移动的。
- 对于每个移动的组，其所有成员也是移动的。

如果源域是本机模式域，全局组还可以包含其它全局组。这意味着每个嵌套组的所有的成员和所有的有成员在那个嵌套组中的全局组必须是移动的。

移动配置文件和 SIDhistory

当制定域重组规划时，必须注意到迁移的用户接收新 SID，这会影响它们的配置文件的使用。在迁移之后登录到它们的计算机的用户会失去对它们的登录配置文件的访问权限，因为它们的主 SID 会发生改变而它们的旧的配置文件可能仍储存在它们的旧的主 SID 中。这会在下列情况下发生：

- 用户是从 Windows NT 域复制的。
- 用户是从 Windows 2000 域复制的。
- 用户是从 Windows 2000 域复制的，但仍在 Windows NT Workstation 登录。

如果用户失去对它们的登录配置文件的访问权限，有两个方案可使配置文件可用于迁移的用户：复制配置文件或共享配置文件。首选方法是复制配置文件。

复制配置文件

第一个方案是将原始的配置文件从其以用户原始的 SID 命名的关键字下的当前位置复制到以用户的新 SID 命名的关键字中。每个帐户都与其自己的配置文件的分开的副本关联。对一个配置文件的更新不反映在另外一个配置文件上面。

使用这种方法的优点是 Windows 2000 行为更可预测。因为数据在配置文件之间不共享，没有可能一个配置文件访问这样的帐户：该帐户具有只适合于另一个域或目录林的另一个帐户的数据。

使用这种方法的缺点包括：它

- 因为储存两个配置文件，消耗额外的磁盘空间。
- 产生难以预料的回退结果。必须彻底地测试安装使用组策略的应用程序的影响以使您对任何偶然事故有备无患。

共享配置文件

这个方案使相同的配置文件可用于用户的原始的帐户和新帐户两种情况。在这些情况下，配置文件的一个副本被两种帐户访问和更新。使用这种方法的优点包括：

- 在用户登录到一个帐户时对配置文件更新（例如，对“ 我的文档 ”的修改、快捷方式等等），在用户随后登录到另一个帐户时仍可以使用。
- 因为只需储存配置文件的一个副本，所以能节约磁盘空间。

使用这种方法的缺点是有未知的变数会影响其使用。例如，如果您创建一个包含组策略引用的新 Windows 2000 帐户配置文件，必须测试回到组策略不同的或没有使用的源帐户的影响。

移动计算机

因为共享本地组和域本地组只在它们被创建的域内有作用域，移动这样的组会将不能解决的任何引用留给源域 ACL 中的组。

在此情况下，一个封闭的计算机和共享或域本地组的集合是这样一个集合，在其中有下列情况存在：

- 对于每个移动的计算机，所有在计算机资源中的 ACL 中被引用的共享或域本地组也移动。
- 对于每个移动的组，包含引用组的 ACL 的域中的所有的计算机也移动。

对移动存在的全局组和封闭的集合的限制是特别严格的。增加和减少大的全局组是费时的。在一些情况下，可以获得的最小的封闭的集合是整个源域。解决这个问题的三个可能的方法包括：

1. 在目标域中为每个待移动的组创建平行全局组，然后找出包含引用原始的组的 ACL 的企业的所有的资源，并将它们重新许可以包括对平行组的引用。

   当移动全局组时，这种方法在以下几个情况中很可能是很复杂的任务：

   - 在任何信任域中的资源中组被引用时。
   - 带有来自本机模式源域的域本地组，其中域本地组可用于域中的任何计算机。

2. 将源域切换到本机模式，然后将组的类型改变以移到通用组。因为通用组在整个目录林中都有作用域，将组改变为通用组意味着它们可以安全地移动，同时仍可维护对留下的资源的访问权限。

   在使用这种方法时一定要小心，因为通用组成员储存在 GC 中，后者存在 GC 复制通讯量的问题。有鉴于此，在用户和组迁移到新域时,必须将这种方法严格地作为过渡策略使用。在迁移完成之后，可以将组回到它们的原始的类型。

3. 将来自源域的组复制进目标域中，同时保留它们的 SIDhistory。这种技术有一些限制，将在本章稍后的“ 复制安全主管 ”中介绍。

移动成员服务器

在上面的举例中，Bob 通过引用计算机本地组 Fin_Files1\Finance Files，并直接引用他的域帐户的 ACL，有权访问成员服务器 Fin_Files1 中的一些资源。

移动域控制器的相关问题包括必须确保维护共享本地组和域本地组，如本章前面所介绍的那样。然而，这些相关问题不同于移动成员服务器（如 Fin_Files）或客户机所涉及的问题。

假设成员服务器移到对 Bob 的新帐户域有信任的域中，SIDhistory 必须确保 Bob 可以访问带有直接引用他的 ACL 的资源。引用计算机本地组的 ACL 也会继续工作，因为组存在于本地计算机的帐户数据库中。这意味着组不受移动的影响，因此其 SID 也不必改变。

建立信任

在域升级时假设从目标域到任何有关系的资源域存在足够的信任,以使到资源的访问权限得以维护。然而，此类信任必须首先在任何域重组方案中建立。

Netdom 是一个用于执行列举域信任和建立新信任之类的任务的工具。这种工具也可用于创建计算机帐户和更新客户机或服务器的域成员。

复制安全主管

到这时，重组都与移动安全主管有关。移动安全主管可在目标域中创建新的完全相同的帐户并删除源域中的帐户。如果迁移发生问题，移动操作不允许返回到旧的帐户状态。

为确保您可以在先导测试项目或生产迁移时摆脱问题而得以恢复，建议您逐步将用户迁移到 Windows 2000 域，同时在源域中维护旧的帐户。这通过“复制”是有可能的，复制是通过使用 ClonePrincipal 工具创建复制用户或组，该工具包含一组 Microsoft Visual Basic (VB) 脚本，执行如复制全局组并复制用户之类的任务。

域重组方案

本节介绍的两种方案能满足域重组的大多数要求。这两种方案都能帮助将用户和计算机从 Windows NT 源域移到 Windows 2000 目标域。示例如下：

- 逐步将用户迁移到 Windows 2000 （在目录林之间）
- 将资源迁移进 Windows 2000 OU（在目录林之间）

方案 1：将用户逐步从 Windows NT 迁移至 Windows 2000

在这种方案中，将用户逐步迁移到原来的 Windows 2000 环境，不会影响 Windows NT 生产环境。图 10.9 是本例的图解。逐步迁移所要求的步骤和工具在本节介绍。

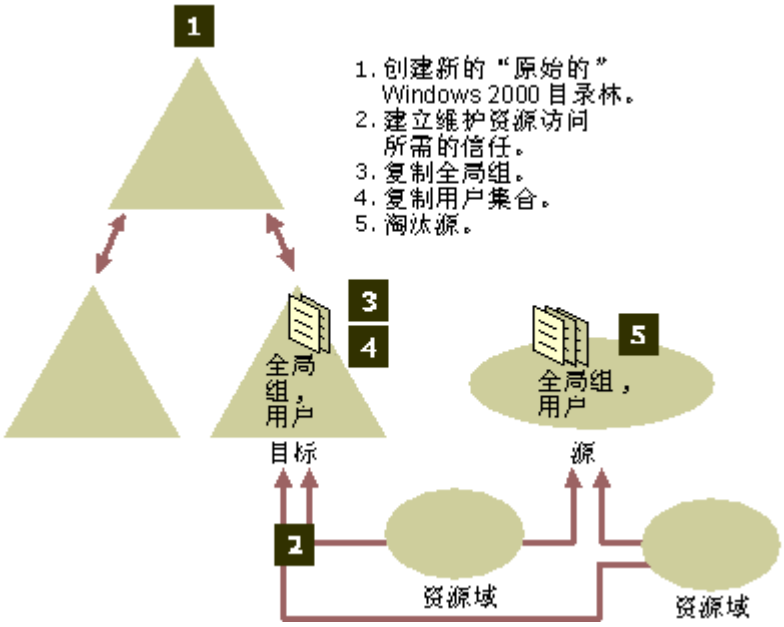


图 10.9 逐步迁移用户

备注　保护当前生产环境免受迁移改变的影响能确保它在本过程中保持完好无损。如果需要，这将允许您还原到旧的生产环境。

在迁移完成之后，可以淘汰旧的帐户域并重新指派域控制器。然后执行以下几个步骤：

1. 创建原始的 Windows 2000 目录林。使用标准过程创建 Windows 2000 目标目录林，以反映本单位的名称空间规划活动中的标识的要求和结构。在新目录林中创建的域将是本机模式 Windows 2000 域。

2. 建立目录林所要求的信任以维护资源访问。这涉及使用 Netdom 查询从任何资源域到 Windows NT 源域中当前存在什么信任。

   然后可以将 Netdom 的输出与允许到目标域中的用户和组资源访问所要求的信任列表进行比较。然后使用 Netdom 建立还没有存在的任何信任。

3. 在目标域中复制所有的源全局组。大多数资源可以使用引用全局组的 ACL 得到保护，通常是间接地通过共享或计算机本地组进行。在建立信任之后，必须确保有关的全局组在目标域中可用。

   完成这件事的最简单的方法是使用 ClonePrincipal 复制所有的全局组。

4. 标识和复制用户集合。在将源全局组复制到目标域之后，可以开始执行迁移用户的任务。

   这是一个反复的任务，因为在大多数情况下您想移动用户集合，这涉及标识要迁移的用户集合，然后使用 ClonePrincipal 复制目标域中的源用户。

5. 淘汰源域。当所有用户和组都永久地移到目标目录林之后，最后的任务是淘汰源域。这涉及首先关闭和删除源域 BDC，然后是源域 PDC。建议储存 PDC 以便用于灾难恢复。

   如果您计划将这些域控制器用于在新目录林中重新指派，可以将它们升级到 Windows 2000 然后再将它们升级到域控制器或者将它们作为成员服务器。

特别是在用户迁移阶段，在每次迁移时测试某些用户的登录也许是明智的。如果在淘汰之前的任何阶段发生错误，可以挂起过程，在源生产域中的工作可以继续。

方案 2：将资源域合并到 OU

在本例中，将资源域合并进本机模式 Windows 2000 域内部的 OU。这样做可以降低管理复杂信任的费用。图 10.10 是本例的图解。逐步迁移所要求的步骤和基本工具在本节介绍。

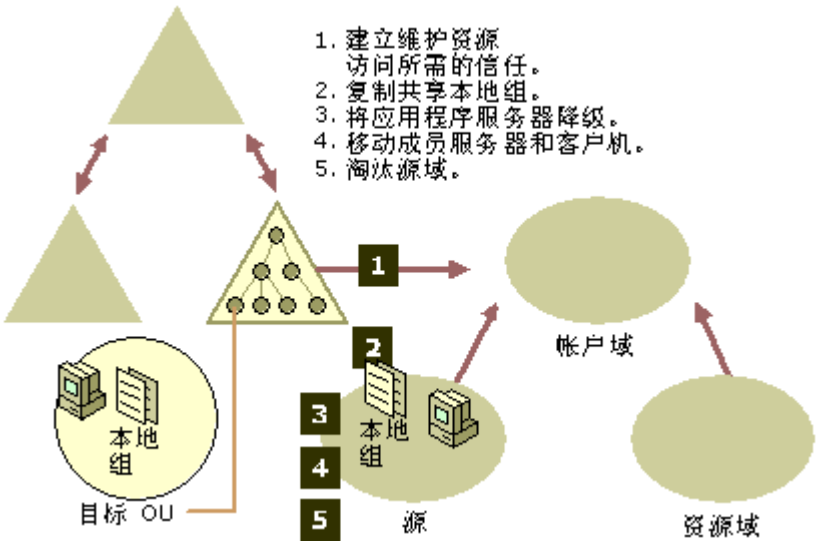


图 10.10 将资源域合并进 Windows 2000 OU

在本例中，应用程序服务器变成目标 OU 中的成员服务器。假设每个域中的应用程序服务器使用共享本地组。还假设域包含一些成员服务器和客户机。

在域重组完成之后，可以淘汰旧的域。将资源域合并进 Windows 2000 OU 的过程如下：

1. 建立从目标域到目录林外部的帐户域所要求的任何信任。这涉及使用 Netdom 查询从任何资源域到帐户域中当前存在什么信任。然后可以将 Netdom 的输出与从目标域到帐户域已经存在的信任进行比较。然后使用 Netdom 建立还不存在的任何信任。

2. 复制所有的共享本地组。共享本地组只在它们被创建的域内部有作用域，并只在该域的域控制器之间共享。不必立即将所有的域控制器移到目标域。为确保维护资源访问同时域控制器和资源在源和目标域之间进行拆分，必须使用 ClonePrincipal 将共享本地组复制到目标域。

3. 将应用程序服务器降级为成员服务器。在复制所有的共享本地组之后，可以开始将应用程序服务器转换为目标 OU 中的成员服务器。

   将资源域的 PDC 升级到 Windows 2000 并在过渡期在混合模式下运行域。然后可以升级每个待降级的 BDC。在 BDC 升级时，运行 Active Directory 安装向导并选择使 BDC 成为成员服务器。

   如果升级 PDC 不可能或不希望，对于每个升级必须使 BDC 脱机并将它升级到 PDC。在将 BDC 升级到 PDC 之后，便可以升级到 Windows 2000，实际使脱机域控制器成为“复制” Windows 2000 混合模式域中的 PDC。在脱机升级 PDC 之后，可以运行 Active Directory 安装向导将 PDC 降级为成员服务器。然后将成员服务器加入到目标域。

4. 移动成员服务器（包括以前的 BDC）和客户机。在此步骤过程中可以使用 Netdom 在目标域 OU 中为待移动的成员服务器或客户机创建计算机帐户。将计算机加入到目标域。

5. 淘汰源域。当所有的组和计算机永久地移到目标目录林之后，最后的任务是淘汰源域。这涉及首先关闭和删除源域 BDC，然后是源域 PDC。

如果计划重新指派新目录林中的源域控制器，可以将它们升级到 Windows 2000。然后可以将它们升级到 Windows 2000 域控制器或者将它们作为成员服务器。

备注 对于这种方案，当将 BDC 降级为成员服务器时，必须尽快将它们移到目标域。除非域在本机模式下，共享本地组转换到域本地组，通过这些组可访问的资源在成员服务器中将不可用。

域迁移工具

本节包含关于本章其它地方引用的域迁移基本工具和 *Windows 2000 Server Resource Kit* 工具的一般信息。功能和使用的权威资料在每一小节列出的源信息中可以找到。

ClonePrincipal

ClonePrincipal 是包括以下几个 COM 对象和示例脚本的工具。可以使用 Visual Basic 自定义脚本。

DSUtils.ClonePrincipal，支持三个方法的 COM 对象：

- **AddSidHistory -** 将源主管的 SID 复制到现有的目标主管的 SIDhistory 中。
- **CopyDownlevelUserProperties -** 将源主管的 Windows NT 属性复制到目标主管中。
- **Connect -** 建立与源和目标域控制器的已验证身份的连接。

通过 ClonePrincipal 可逐步将用户迁移到 Windows 2000 环境，而不影响现有的 Windows NT 生产环境。这可通过在 Windows 2000 环境中创建 Windows NT 用户和组的复制本来完成。以这种方式使用 ClonePrincipal 的优点如下：

- 用户可以登录到目标帐户（复制）也能在试验期间紧急回退到源帐户。
- 同时可以将好几个用户引入到目标 Windows 2000 环境。
- 当用户迁移到目标 Windows 2000 环境时，源生产环境不会分裂。
- 不必更新 ACL 以保留目标帐户的组成员和网络访问。
- 不同源域的具有相同名称或目的多个组可以“合并”进相同的目标对象。

另外，可以通过使用 ClonePrincipal 复制本地组，将大量的小的资源域合并进 Windows 2000 OU。

备注 AddSidHistory 方法是对安全敏感的操作，具有以下几个限制：

- AddSidHistory 要求具有或提供源和目标域中的域管理员凭据。源和目标域决不能在相同的目录林中。尽管在源和目标域之间存在外部信任，这种功能不需要这样的信任。

- 可以审查 AddSidHistory 事件，这能确保源和目标域管理员可以发现执行这种功能的时间。在源域可以推荐做审查，但不要求这样做，而在目标域中要使 AddSidHistory 成功必须启用审查。

- ClonePrincipal 示例脚本调用基础 AddSidHistory 方法，因此其它 ClonePrincipal 工具与 AddSidHistory 受相同的安全灵敏度和限制的制约。

Netdom

Netdom 是允许您从命令行管理 Windows 2000 域和信任关系的工具。

使用 Netdom 执行下列任务：

将 Windows 2000 计算机加入到 Windows NT 或 Windows 2000 域，并：

- 提供一个选项为计算机帐户指定 OU。
- 为最初的加入产生随机计算机密码。

为域成员客户机和成员服务器管理计算机帐户：

- 添加、删除和查询。
- 提供一个选项为计算机帐户指定 OU。提供一个选项为成员客户机将现有的计算机帐户从一个域移到另一个域并维护该计算机帐户上的安全描述符。

在域之间建立（单向或双向）信任关系，包括下列域类型的信任：

- Windows NT 域。
- 域树中的 Windows 2000 父域和子域。
- 链接到 Kerberos 领域的信任的 Windows 2000 部分。

为下列配置检验和重新设置安全通道：

- 成员客户机和服务器。
- Windows NT 域中的 BDC。
- 特殊的 Windows 2000 副本。

管理域之间的信任关系

- 查看所有的信任关系。
- 列举直接的信任关系。
- 列举所有的（直接的和间接的）信任关系。

迁移规划任务列表

表 10.7 是涉及迁移规划的任务小结。

表 10.7 迁移规划任务小结

任务	所在章节
确定迁移路线图。	开始迁移规划过程
确定受支持的升级途径。	规划域升级
检查现有域结构。	规划域升级
制定恢复规划。	规划域升级
确定升级域控制器的策略。	规划域升级
确定升级域的顺序。	规划域升级
确定切换到本机模式的时间。	规划域升级
确定重组域的理由。	规划域重组
确定重组域的时间	规划域重组
移动用户和组。	规划域重组
移动计算机。	规划域重组
移动成员服务器。	规划域重组
建立信任。	规划域重组
复制安全主管。	规划域重组
切换到本机模式。	规划域升级 规划域重组

第 11 章 - 规划分布式安全

安全规划是您 Microsoft® Windows® 2000 部署规划的一个基本组成部分。此任务中将涉及到许多您的部署子组的代表。本章向您介绍在 Windows 2000 网络中规划分布式安全的一个策略。它概述了分布式安全的主要目标，并介绍了 Windows 2000 的安全策略。

本章将把为有效使用 Windows 2000 安全所需予以考虑的重要因素置于上下文中。然而，分布式计算机安全是一个相当复杂的课题，需要进一步研究。

本章内容

制定网络安全规划
验证所有用户访问权限
应用访问控制
建立信任关系
启用数据保护
设置统一安全策略
部署安全应用程序
管理事务
分布式安全的规划任务列表

本章目标

本章将帮助您制订下列规划文档：

- 安全风险分析
- 安全策略
- 安全组说明及关联策略
- 网络登录及身份验证策略
- 信息安全策略
- 管理策略

资源工具包中的相关信息

- 有关分布式安全的详细信息，请参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide*。
- 有关安全组的详细信息，请参见本书中的“设计 Active Directory 结构”。
- 有关公钥基础结构的详细信息，请参见本书中的“规划公钥基础结构”。

制定网络安全规划

分布式安全涉及到对计算机网络中多个安全功能的协调来实现一个总体的安全策略。分布式安全使用户可以登录适当的计算机系统、查找所需信息并使用之。计算机网络上的许多信息对每个人都可读，但只有很少一部分人才可以对它更新。如果信息是敏感或专用的，则只允许被授权的个人或组读这些文件。对在公用电话网、Internet、甚至公司内部网段上传输的信息的保护及其隐私权也是一个要考虑的问题。

虽然安全技术是一些非常先进的技术，但安全本身融合了这些技术和良好的商业及社会实践方案。不管这些技术是如何先进、实现得如何好，它只不过同采用和管理它的那些方法一样好。

您的安全部署组制定网络安全规划。网络安全部署规划说明了如何使用 Windows 2000 分布式安全功能来部署分布式安全及信息安全解决方案。一个典型的安全规划包含如表 11.1 所示的部分。

表 11.1 安全规划的各部分

规划的各个部分	说明
安全风险	列举影响您企业的安全危险的类型
安全策略	说明应付此风险所必须的常规安全策略。
公钥基础结构策略	包含您为内部或外部安全功能而部署证书颁发机构的规划。
安全组说明	包含对安全组及其相互之间关系的说明。这个部分将组策略映射到安全组。
组策略	包含您如何配置安全组策略设置，比如说网络密码策略。
网络登录及身份验证策略	包含为登录网络以及为使用远程访问和智能卡登录所需的身份验证策略。
信息安全策略	包含您如何实现信息安全解决方案，例如安全电子邮件和安全 Web 通信。
管理策略	包含委派管理任务和监视审核日志以检测可疑活动的策略。

您的网络安全部署可以包含更多的部分，但是，以上这些是所建议的最少部分。另外，您的单位可能需要不止一个安全规划。规划的个数取决于您的部署范围。一个国际组织可能需要为其每个重要分部或地区制定一个规划，而一个区域性组织则可能只需要一个规划。对不同用户组有截然不同的策略的单位可能对其每个组都需要一个网络安全规划。

通过使用代表您单位计算环境的测试实验室来测试和修改您的网络安全规划。另外，用先导测试程序来进一步测试并改进您的网络安全规划。

安全风险

在本章讨论 Windows 2000 的安全功能以前，复习一下 IT 经理所面临的网络安全问题的类型是一个不错的主意。表 11.2 说明了几种安全风险的类型，并为后面对安全功能、策略、以及技术的讨论提供了一个共同的基础。在您的安全规划中创建一个与此相似的列表可以说明你面临的安全问题的复杂性，并会帮助您为风险的各种类型建立一套标准标签。

表 11.2 一个单位的安全风险类型

安全风险	说明
标识截取	入侵者发现一个合法用户的用户名和密码。这可以通过多种方法达到，社会的和技术的方法都有。

冒名访问	一个非法用户伪装成一个合法用户。例如，一个用户擅用信任系统中的 IP 地址并以此获得对赋予被模拟设备或系统的访问权。
重复攻击	入侵者记录用户和服务器之间的网络交换并在以后回放之以模拟该用户。
数据截取	如果数据以明文方式通过网络，则未经授权的用户可以监视并捕获此数据。
操纵	入侵者造成网络数据的修改或损坏。未经加密的网络金融事务易受操纵。病毒可以破坏网络数据。
否认	如果事务的接收者不能确定是谁送出消息的，则会危及到基于网络的商业或金融事务。
宏病毒	与应用程序有关的病毒能够利用复杂文档和电子数据表的宏语言。
拒绝服务	入侵者使用消耗系统资源的请求来淹没服务器，使其崩溃或不能完成有用的工作。服务器系统崩溃有时会为渗透系统提供机会。
恶意移动代码	这个术语是指从 Internet 上载到 Web 服务器的作为自动执行的 ActiveX® 控件或 Java Applet 运行的的恶意代码。
滥用特权	一个计算系统的管理员故意或错误地使用对该操作系统的特权来获得私有数据。
特洛伊木马	这是对一种伪装成令人想要的无害工具的恶意程序的一种通用术语。
社会工程攻击	有时闯入网络简单得就如叫过一个新员工，告诉他你是 IT 部门来的并要求他们验证密码供您记录那样。

安全概念

以下的概念对描述 Windows 2000 下的分布式安全策略有用。您也许还会发现将其放入您的安全规划以使您的读者熟悉分布式安全也是有用的。

安全模型

Windows 2000 安全基于一个使用 Microsoft® Active Directory™ 目录服务的身份验证和授权的简单模型。当用户登录和建立与服务间的网络连接时，身份验证识别用户。一旦验证后，用户就根据权限被授权访问一组特定的网络资源。授权是通过访问控制的机制，使用定义对文件、系统、网络文件和打印共享、以及 Active Directory 的项目的权限的访问控制列表 (ACL)来进行的。

域模型

Windows 2000 中，域是一组在安全方面共享目录数据库的网络对象的集合，例如用户帐户、组、以及计算机。域标识一个安全颁发机构并形成一个安全边界，拥有一致的内部策略和与其他域之间的明确关系。

信任管理

信任是域之间建立的一种逻辑关系，其目的是允许传递身份验证，在身份验证中信任域认可受信域的登录身

份验证。术语可传递信任是指通过一个信任关系链的身份验证。为了后向兼容，在 Windows 2000 中，信任关系支持跨域的身份验证，这是用 Kerberos v5 协议以及 NTLM 身份验证来实现的。

安全策略

安全策略设置定义系统的安全行为。通过对 Active Directory 中组策略对象的使用，管理员可以将明确的安全配置文件集中应用到企业中各种计算机类别上。例如，Windows 2000 有一个称为“**默认域控制器策略**”的默认组策略对象，它决定域控制器的安全行为。

安全配置与分析

安全配置与分析是 Windows 2000 的一项功能，它提供了将一个计算机的安全设置与标准模板相比较、查看结果、并解决由分析所揭示的任何差异的能力。您也可以导入一个安全模板到一个组策略对象并将此安全配置文件同时应用到多台计算机。Windows 2000 包含几个预定义的安全模板，适合于各种安全级别和网络中不同类型的客户机和服务器。

对称密钥加密

亦称为密钥加密，对称密钥加密用相同的密钥来对数据进行加密和解密。它提供了对数据的快速处理能力并被用于网络和文件系统数据加密的多种形式。

公钥加密

公钥加密有两个密钥，一个公钥和一个私钥。每个密钥都可以加密只能由另一个密钥解密的数据。这种技术提供了多种的安全策略，它是几种 Windows 2000 安全功能的基础。这些功能依赖于公钥基础结构 (PKI)。有关 PKI 的详细信息，请参见本书中的“规划公钥基础结构”。

身份验证

身份验证确认任何试图登录一个域或访问网络资源的用户的身份。Windows 2000 身份验证对所有网络资源启用单一登录。使用单一登录，用户可以用一个密码或智能卡一次登录到客户计算机即为该域中任何计算机所验证身份。Windows 2000 中的身份验证是用 Kerberos v5 协议、NTLM 身份验证、或登录 Windows NT 4.0 域的 Windows NT 登录功能来实现的。

单一登录

用户不喜欢必须对多个网络服务器和应用程序分别进行身份验证。用户对登录本地计算机、访问一个文件或打印服务器、发送一封电子邮件、或者使用数据库等等可能必须分别提供密码。不同的服务器可以不同时间间隔要求更改密码，而且通常不允许重用，因此一个典型的用户可能会要记住半打密码。不仅仅身份验证对用户来说枯燥无味，而且同时用户还开始写下当前的密码列表。这样，多身份验证网络可能会易于受到标识截取的攻击。

单一登录策略使得用户可以进行一次交互式的身份验证，然后就可以以已验证的状态登录到其他网络应用程序和设备了。这些后续的身份验证事件对用户是透明的。

两因素身份验证

两因素身份验证要求用户提供一个对其身份和密码进行编码的物理对象。两因素身份验证最常见的例子是自动柜员机 (ATM) 卡，ATM 卡要求一个个人识别码 (PIN)。

生物统计标识是两因素身份验证的另一种形式。一个特殊设备扫描用户的手印、拇指指纹、虹膜、视网膜、或声波纹而不是访问卡。然后用户输入密码的对等信息。这种方法价格昂贵，但是它使得标识截取和冒名访问十分困难。

对商业企业来说，正在兴起的两因素技术是智能卡。这种卡不比 ATM 卡大多少，可由用户带在身上。它包含一个储存数字证书和用户私钥的芯片。用户将卡插入客户机的读卡器后输入一个密码或 PIN。由于私钥是在用户兜里的卡上，网络入侵者很难偷取。Windows 2000 直接支持智能卡身份验证。

访问控制

访问控制是实现授权的模型。在用户通过了域的身份验证并试图访问资源（例如一个网络文件）时，所允许的操作的类型取决于属于此资源的权限，比如说只读或读/写。Windows 2000 中的访问控制通过使用与对象有关的 ACL 来实现。可以在文件或文件夹属性页的“ 安全 ”选项卡中查看 ACL。该列表包含拥有对该对象的访问权的用户组名称。

数据整体性

确保数据整体性意味着保护数据免受恶意的或意外的修改。对存储起来的数据，这意味着只有被授权的用户才能编辑、重写、或删除数据。在网络中，这意味着数据包必须包含某个数字签名以便接收计算机可以检测到对数据包的篡改。

数据机密性

数据机密性策略意味着在数据通过网络之前对其加密并在之后对其解密。这个策略防止了数据被被网络上的窃听者读取（数据截取）。一个通过网络传输的未加密数据包可以很容易地被网络上的任何一台计算机用一个数据包监探程序看到，这个数据包监探程序是从 Internet 上下载的。

认可

认可策略有两个部分。第一个是确定一条消息由一特定用户发送，该用户不能否认之。第二个部分是确保消息不能是由任何模拟该用户的人发送的。

这是公钥基础结构的又一个应用程序。用户的私钥用来在消息中放入一个数字签名。如果接收者可以用发送者的公钥读取该消息，则该消息只能是由这个特定的用户发送的，而不会是别的人。

代码身份验证

这个策略要求从 Internet 上下载的代码由受信软件发行者的数字签名进行签名。您可以配置 Web 浏览器来避免运行没有签名的代码。注意软件签名证明该代码是可信的，即表示它在发布后没有被篡改过。它并不保证该代码是可以安全运行的。您必须决定相信哪个软件发行商。（可执行文件上的数字签名是公钥基础结构的另一个例子。）

审核日志

审核用户帐户管理和对重要网络资源的访问是一项重要的安全策略。审核留下网络操作的跟踪记录，说明由谁进行了什么尝试。这不仅有助于检测到入侵，而且一旦入侵者被抓获和起诉，该日志便成为法律证据。最后，查找以及删除或修改审核日志的工作对这个老练的入侵者造成了一项额外的耗时的任务，使得探测和干涉更为容易。

物理安全

不用说，关键的企业网络服务网络需要置于锁定的设备当中。如果入侵者可以坐在网络服务器控制台前面，他们可能会控制该网络服务器。如果关键的网络服务器物理上不安全，则一个心怀不满的雇员可以用一个简单的老式工具（比如说铁锤）破坏您的硬件。您的数据也可遭受到物理攻击的损害。每个新手都知道如何按删除键。这样的入侵所造成的破坏也能导致和更为老练的外来攻击所造成的破坏同样多的数据丢失和停机时间。对网络的攻击不必复杂也能有效。

用户教育程度

对社会工程攻击最好的防卫是教您的用户保持其密码机密和安全。必须清楚明白地说明关于分发关键信息的商业策略。发行一个安全策略并要求所有人遵守。教育的一种方法是举例。确保您的 IT 专业人员保护他们的密码并且确保他们鼓励用户保护其密码。

分布式安全策略

分布式安全是指主要在企业网络内部操作的逻辑安全功能。要使您的网络资源安全，有七种主要安全策略要推行。

- 对所有访问系统资源的用户进行身份验证。
- 对所有资源应用适当的访问控制。
- 在多个域之间建立适当的信任关系。
- 对敏感数据启用数据保护。
- 设置统一的安全策略。
- 部署安全应用程序。
- 管理安全管理。

这七个主题应作为您的分布式安全规划的中心。在后面有对每种策略的深入讨论。

验证所有用户访问权限

要为您的 Windows 2000 提供安全性，必须为合法用户提供访问权而屏蔽掉试图侵入的入侵者。这意味着您必须设置您的安全功能来验证所有用户对系统资源的访问。身份验证策略设置防止入侵者盗取标识或模拟用户的保护级别。

Windows 2000 中，对域用户的身份验证基于 Active Directory 中的用户帐户。系统管理员使用 Microsoft 管理控制台 (MMC) 的 Active Directory 用户和计算机管理单元来管理这些帐户。用户帐户可以被组织到称为“ 组织单位 ”的容器中，这些“ 组织单位 ”反映您的 Active Directory 名称空间设计。用户帐户的默认位置是该管理单元的“ 用户 ”文件夹。

当新用户加入该组织时，管理员只为该用户创建一单个的帐户而不是必须在不同服务器和应用程序数据库中创建半打或者更多的个别帐户。由于域身份验证服务和企业目录集成到一起，该单个用户帐户不仅提供对所有网络服务的访问，也是一个全局地址薄信息的目录项目。用户可以只用一个密码在域中不同客户计算机或膝上电脑上登录。

Windows 2000 自动支持域目录林中用户的单一登录。按默认方式，目录林中的域信任关系是双向的。因此，对目录林中其他域中的资源的引用或传递身份验证来说，在一个域中的身份验证已经足够了。用户在会话开始时交互式地登录，然后网络安全协议（Kerberos v5 协议、NTLM、以及安全套接字层/传输层安全）就向所有被请求的服务透明地证明该用户的身份。

Windows 2000 可支持对强身份验证的智能卡登录，这是可选的。智能卡是由用户携带的用来在交互式登路中代替密码的标识卡。它也可以用于远程拨号网络连接和作为一个保存用于安全套接字层（SSL）客户身份验证或安全电子邮件的公钥证书的地方。

身份验证不仅限于用户。计算机和服务在建立到其他服务器的网络连接时也要通过身份验证。例如，基于 Windows 2000 的服务器和客户计算机在启动时连接到其域的 Active Directory 以获取策略信息。在任何用户可以登录到该计算机以前，它们向 Active Directory 验证身份并从 Active Directory 下载计算机策略。计算机和服务也向要求相互认证的客户证明其身份标识。相互认证防止入侵者在客户和真实的网络服务器之间添加另外一台计算机作为冒名者。

计算机和服务可以进行“ 受信委派 ”，即服务可以“ 代表 ”用户建立另一条网络连接而不必知道用户的密码。在服务可以为该用户建立到另一台计算机的新的网络连接之前，用户必须已经和服务之间有了一条相互验证过的网络连接。这对为使用多台计算机的单一登录能力而设计的多层应用程序是有用的。这个功能在运行于文件服务器的加密文件系统 (EFS) 环境下尤其有用。要用一个服务来委派一条网络连接，请使用 Active Directory 用户和计算机 MMC 管理单元。然后在属性页中选中“ 信任计算机委派 ”复选框。

规划的注意事项

规划身份验证策略时，请一定要考虑以下注意事项和最佳实现方案。

对抗暴力或字典密码破解工具的最简单方法是建立并实行长而复杂的密码。Windows 2000 让您设置策略来管理用户密码的复杂性、长度、生存时间以及可重用性。一个复杂的密码有十位或更多的字符，包含大写和小写字母、标点符号以及数字。一个复杂密码的例子："My,Birthday,Is,623"。

智能卡提供了比密码强得多的身份验证，但是也带来了额外的费用。智能卡要求配置 Microsoft 证书服务、智能卡读取器设备以及智能卡本身。有关部署智能卡的详细信息，请参见本章后面的“ 智能卡登录 ”和本书中的“ 规划公钥基础结构 ”。

注意第三方供应商提供了许多安全产品来提供两因素身份验证，包括“ 安全令牌 ”和生物统计附件。这些附件使用可扩展的 Windows 2000 图形化登录用户界面功能来提供另一种用户身份验证的方法。

“ 信任计算机委派 ”是一种非常强大的能力。它不是默认启用的，而是需要域管理员特权才能将其对特定计算机或服务帐户启动。对被信任作为委派的计算机或帐户的访问需要加以限制以防止引入特洛伊木马程序，这些特洛伊木马程序会滥用为用户建立网络连接的能力。

一些帐户可能会太过敏感而不能允许委派，即使是由受信服务器委派也不行。您可以设置单独的用户帐户以使得它们不能被委派，即使服务是被信任为可委派的也不行。要利用这个功能，请到 Active Directory 用户和计算机 MMC 管理单元并打开该帐户的属性页。在这张属性页的“ 帐户 ”选项卡中查找“ 帐户敏感不可委派 ”复选框。

Kerberos 身份验证和信任

Kerberos 身份验证协议是对单一登录到网络资源的一种技术。Windows 2000 使用 Kerberos v5 协议来提供对域中网络服务和对处于受信域中的服务的快速单一登录。Kerberos 协议验证用户和网络服务的身份，提供相互认证。

Kerberos 身份验证工作原理

用户输入域凭据（通过用户名和密码或智能卡登录）后，Windows 2000 定位一个 Active Directory 服务器和 Kerberos 身份验证服务。Kerberos 服务发给用户一张“票据”。这是一个包含用于向网络服务器标识用户的信息的证书。初始交互式登录后，用第一张 Kerberos 票据来请求其他的 Kerberos 票据以登录后面的网络服务。这是一个复杂的过程并且还涉及到了用户和服务器之间的相互身份验证，但是它对用户却是完全透明的。（有关 Kerberos v5 身份验证的详细信息，请参见 Windows 2000 Server “帮助”。）

Kerberos 身份验证减少了用户需要记忆的密码数目，因此也就减小了标识截取的危险。目录林中的域之间的信任关系将 Kerberos 身份验证的使用范围扩大到了许多网络资源。

实现 Kerberos 身份验证

实现 Kerberos 身份验证没有前提条件。Kerberos 协议广泛用于 Windows 2000 中。您不需要安装或启动之。

对 Kerberos 安全策略参数可以在 MMC 组策略管理单元中设置。在组策略对象内，Kerberos 设置位于帐户策略下。

组策略对象
X 计算机配置
X Windows 设置
X 安全设置
X 帐户策略
X Kerberos 策略

这些设置必须只能为熟悉 Kerberos 协议的合格管理员所使用。

Kerberos 安全的注意事项

要从 Kerberos 身份验证的增强性能和安全性中充分受益，请考虑将 Kerberos 登录作为贵企业唯一的网络登录协议。Windows 2000 为实现跨平台互操作性使用 Kerberos v5 身份验证协议的 IETF 标准版本。例如，UNIX 系统用户可以用 Kerberos 凭据登录到 UNIX 系统并安全地连接到 Windows 2000 服务以访问由 Kerberos 身份验证所启用的应用程序。对已经使用基于 UNIX 领域的 Kerberos 身份验证的企业网络来说，可以用 Kerberos 名称映射来创建和 Windows 2000 域之间的信任关系并为 UNIX 帐户集成 Windows 2000 身份验证。

注意在由 Kerberos 进行身份验证的网络上的计算机通常必须将其时间设置与一个公用时间服务同步，时差不超过五分钟，否则身份验证会失败。Windows 2000 计算机自动以域控制器作为网络时间服务对当前时间进行更新。域控制器以该域的主域控制器为权威时间服务。即使域中或跨域的各计算机当前时间不一样，Windows 2000 也会自动处理时钟差避免登录问题。

当在目录林中的域之间使用可传递的信任时，Kerberos 服务搜索域间的信任路径以创建一个跨域引用。

在大的目录树中，在跨域交互作用程度高的域之间建立双向信任交叉链接可能更为有效。这允许更快的身份验证，因为当产生引用消息时，它给予 Kerberos 协议可以遵循的“快捷方式”。

Kerberos 身份验证在一个目录林中的域之间使用透明的可传递的信任，但它不能在分离的域目录林中的域之间进行身份验证。要使用一个分离目录林中的资源，用户必须提供登录该域目录林中的域的有效凭据。作为另一种可选方案，如果存在一种单向的信任关系则应用程序将使用 NTLM 身份验证，如果安全策略允许的话。

Windows 2000 仍然维持了与 NTLM 身份验证协议的兼容性以支持与 Microsoft 操作系统老版本之间的兼容。您可以对 Microsoft® Windows® 95、Microsoft® Windows® 98、Microsoft® Windows® NT 4.0 Server、以及 Windows NT 4.0 Workstation 客户继续使用 NTLM。NTLM 身份验证也被针对明确要求 NTLM 安全设置的 Windows NT 早期版本的应用程序用在 Windows 2000。

智能卡登录

Windows 2000 支持可选的智能卡身份验证。智能卡提供了一种十分安全的用户身份验证、交互式登录、代码签名、以及安全电子邮件的方法。然而，部署和维护一个智能卡程序需要额外的资源和成本。

智能卡工作原理

智能卡包含一个保存有用于多种目的的用户私钥、登录信息、以及公钥证书的芯片。用户将卡插入与计算机相连的智能卡读取器中。然后用户在被要求时键入一个个人识别码(PIN)。

智能卡通过电路板上的私钥存储提供防篡改身份验证。私钥则用于提供与数字签名和加密相关的其他安全的形式。

智能卡直接实现了一个两因素身份验证策略，并间接允许多个应用程序的数据机密性、数据整体性以及认可，包括域登录、安全电子邮件、以及安全 Web 访问。

实现智能卡的先决条件

智能卡依赖于 Windows 2000 的公钥基础结构 (PKI)。关于 PKI 的详细信息，请参见本书中的“规划公钥基础结构”。

如何实现智能卡

除了 PKI 和卡本身以外，每台计算机还需要一个智能卡读取器。将至少一台计算机设置为智能卡登记站，并授权至少一个用户对它进行操作。这不要求除智能卡读取器以外的其他硬件，但需要对操作登记站的用户颁发登记代理证书。

关于实现智能卡的详细步骤，请参见 Windows 2000 Server “帮助”。

智能卡的注意事项

您需要一个企业证书颁发机构而不是一个独立的第三方证书颁发机构来支持对 Windows 2000 域的智能卡登录。

Microsoft 支持符合工业标准“个人电脑/智能卡 (PC/SC)” (Personal Computer/Smart Card (PC/SC)) 的智能卡和智能卡读取器，并为商业即插即用智能卡提供驱动程序。对 Windows 2000 Professional、Windows 2000 Server、以及 Windows 2000 Advanced Server 系统都支持智能卡登录。随着越来越多的企业用户能够将智能卡用于域身份验证、远程拨号网络访问以及其他应用，使用智能卡的安全优点逐渐为人所认识。

Microsoft Windows 2000 不支持不符合 PC/SC 或不是即插即用的智能卡读取器。一些制造商可能会提供与 Windows 2000 兼容的非即插即用智能卡读取器驱动程序，然而，我们还是建议您只购买即插即用的和符合 PC/SC 的智能卡读取器。

智能卡可以和雇员卡钥以及标识证章结合，以支持一卡多用。

管理智能卡程序的总费用取决于几个因素，包括：

- 登记到该智能卡程序的用户数目及其位置。
- 您将智能卡颁发给用户的具体做法，包括验证用户身份的要求。例如，您是只要求用户简单地出示一张有效个人识别卡呢，还是要求对其背景进行调查？您的策略影响到提供的安全级别，也影响到实际费用。
- 您对丢失或胡乱放置其智能卡的用户的处理方法。例如，您是将临时智能卡发给用户、授权对网络的备用登录呢，还是让用户回家去取他们的智能卡呢？您的策略影响到损失的工作时间以及所需的支持中心的支持服务。

您的网络安全部署规划需要说明您所使用的网络登录和身份验证方法。请在安全规划中包括以下信息：

- 确定您想要采用的网络登录及身份验证策略。
- 说明智能卡部署注意事项及问题。
- 说明支持智能卡所需的 PKI 证书服务。

远程访问

路由和远程访问是让远程用户通过电话连接到您的局域网的服务。本节只讨论路由和远程访问的远程访问安全功能。远程访问从本质来说是对入侵者的邀请，因此 Windows 2000 提供了多个安全功能在限制恶作剧的同时允许授权的访问。

远程访问工作原理

客户拨叫您网络上的一台远程访问服务器。如果满足下列情况，则允许客户访问网络：

- 该请求和对该服务器定义的一个远程访问策略匹配。
- 对该用户帐户启用了远程访问。
- 客户/服务器身份验证成功。

客户已被识别并授权后，根据该客户的远程访问配置文件，可将对网络的访问限制到特定服务器、子网、以及协议类型。否则，对连到局域网的用户所提供的所有典型服务（包括文件与打印共享、Web 服务器访问以及消息传递）都通过远程访问连接启用。

远程访问策略

基于 Windows 2000 的服务器由安全策略控制，这些安全策略决定了它们的远程访问行为。这些策略确定一个服务器是否接受远程访问请求，如果接受的话，是在什么时候、使用什么协议以及要求什么类型的身份验证。

您用 MMC 计算机管理单元定义远程访问的策略。您在远程访问策略节点中定义该策略。

计算机管理（本地）
X 服务及应用程序
X 路由和远程访问
X 远程访问策略

右击控制台树中的一个策略并选择“ 属性 ”。远程访问策略定义为一条带有条件和操作的规则。如果满足条

件，则执行该操作。例如，如果当天的时间适合远程访问、如果所要求的协议是允许的、而且如果所要求的端口类型可用，则允许访问。如果授予了访问权，则远程访问由该策略的访问配置文件所限制。单击“ 编辑配置文件 ”以查看可用配置文件选项。

如何启用远程访问

要对某用户启用远程访问，请打开 MMC Active Directory 用户及计算机管理单元。右击一个用户并选择“ 属性 ”。选择属性页中的“ 拨入 ”选项卡。

关于远程访问以及安装和配置远程访问服务器的详细信息，请参见 Windows 2000 Server “帮助”。关于远程访问身份验证的详细信息，请参见 *Microsoft® Windows® 2000 Server Resource Kit Internetworking Guide* 中的 “Remote Access Server”。

远程访问的注意事项

如果对远程访问服务器没有合适的远程访问策略，则授予远程访问权限给一个用户是无效的。

Windows 2000 对远程访问支持下列身份验证选项：

- 基于用户名和密码的标准点到点协议 (PPP) 挑战响应身份验证方法。

  标准 PPP 身份验证方法只提供有限的安全性。

- 自定义可扩展身份验证协议 (EAP) 身份验证方法。

  可以由第三方开发或提供 EAP 方法来扩展 PPP 的身份验证能力。例如，您可以用 EAP 来提供使用令牌卡、智能卡、生物统计硬件或一次性密码系统的更强身份验证。

- 基于数字证书和智能卡的 EAP 传输层安全 (EAP-TLS) 身份验证。

  EAP-TLS 提供强身份验证。用户的凭据保存在防篡改的智能卡中。您可以向每个用户颁发一张智能卡用于所有的登录。

建议您的网络安全规划包含远程访问和身份验证的策略，包括以下信息：

- 要使用的登录身份验证策略。
- 使用路由和远程访问以及虚拟专用网络的远程访问策略。
- 支持使用数字证书的用户登录身份验证所需的证书服务。
- 为身份验证证书和远程访问登记用户所需的进程和策略。
- 是否使用远程访问回叫以协助消除冒名攻击。

应用访问控制

用户登录后，则被授权访问各种各样的网络资源，例如授权给已验证用户的文件服务器和打印机。一定要将用户的网络资源视图限制到和工作相关的设备、服务、以及目录。这样就限制了入侵者通过模拟合法用户所造成的破坏。

对网络资源的访问是基于权限的。权限确定允许使用特定资源执行特定操作的用户和组。例如，财务组有访

问“ 财务报表 ”文件夹中文件的读/写权限。而审核员组对“ 财务报表 ”文件夹中的文件则只有只读权限。

权限是用和各资源相关联的 ACL 来启用的。您可以在属性页的“ 安全 ”选项卡中找到 ACL。ACL 是一个拥有对该资源的访问权的安全组（在极少的情况下是个人）的列表。

安全组是管理权限的最有效方法。您可以将权限指派给单个用户，但在大多数情况下，将权限授予一个组然后添加或删除该组的成员会更为简单。

Windows 2000 有一个叫做 “Everyone” 的安全组，在创建网络共享的 ACL 后它以默认方式出现于其中。要限制对网络共享的访问，必须删除这个 “Everyone” 组并代之以一个或多个适当的组。不要假定对一个资源的默认权限一定就是合适的。

文件系统权限被默认地赋予了一个叫做 Users 的组。任何通过该域验证的用户都属于称为 Authenticated Users 的组，这个组也是 Users 一个成员。看看资源是干什么用的并确定适当的策略。一些资源是公用的而另一些则需要只对特定的几组人可用。有时，一个大组对一个文件或文件夹有只读权限,而一个更小的组有读/写权限。

访问控制列表

ACL 说明拥有对 Windows 2000 中的特定资源访问权限的组和个人。这些个人和安全组是在 MMC Active Directory 用户和计算机管理单元中定义的。许多类型的 Windows 2000 对象都和 ACL 有关联，包括所有的 Active Directory 对象、本地 NTFS 文件及文件夹、注册表以及打印机。ACL 的控制是如此精细以至于您可以将安全访问限制施加于个别字体上。

ACL 工作原理

访问控制列表实现使用限制策略。Windows 2000 为对许多对象的访问提供了极精细的安全控制。要给予一个组访问某对象的权限，先将该组添加到该对象的 ACL 中。然后您可以调整该组可以施加于此对象的特定权限。例如，对本地文件夹而言，对一个组可用的权限以“ 读 ”、“ 写 ”、“ 修改 ”和“ 删除 ”开始，但这只是十三种可用权限的前四种。

实现 ACL 的先决条件

访问控制列表在 Windows 2000 中非常普遍。唯一的先决条件是 ACL 是安全组和用户的列表。您必须在将其加入 ACL 以前定义那些说明您单位项目或商业角色的组。

如何实现 ACL

对一个对象的访问控制列表通常可在属性页的“ 安全 ”选项卡中找到。这个选项卡显示了拥有对该对象访问权的组的列表以及关于各个组所享有的权限的摘要信息。有一个“ 高级 ”按钮详细显示组权限，这样，用户可以使用授权的更高级功能，比如说定义访问继承选项。

例如，要查看对一个打印机的访问控制列表，单击“ 开始 ”，然后点向“ 设置 ”。点向包含“ 控制面板 ”的文件夹，然后单击“ 打印机 ”。右击一个打印机并选择“ 属性 ”。该打印机的访问控制列表在“ 安全 ”选项卡上。

要想看一个本地文件夹的访问控制列表，打开“ 我的电脑 ”并用 Explore 来导向该文件夹。右击该文件夹。点向“ 属性 ”并单击“ 安全 ”选项卡。

要查看 MMC Active Directory 用户和计算机管理单元中的一个组织单位（文件夹）的访问控制列表，您必须打开“ 查看 ”菜单、选择“ 高级功能 ”。否则，“ 安全 ”选项卡在“ 属性 ”对话框中不可见。

关于访问控制和 ACL 的详细信息，打开 Windows 2000 Server “帮助”并单击“ 索引 ”选项卡。滚动到“ 访问控制 ”。该索引中有许多相关主题，因为 ACL 在整个该产品中随处可见。

安全组

Windows 2000 允许您将用户及其他域对象组织到组当中，以使管理访问权限简单易行。定义安全组是您的分布式安全规划的一个主要任务。

Windows 2000 安全组让您仅用一次操作将同样的安全权限指派给大量的用户。这就确保了一个组中所有用户的安全权限的一致性。使用安全组来指派权限意味着对资源的访问控制保持相当程度的静态并易于控制和审核。根据需要将需要访问的用户添加到适当的安全组当中或从适当的安全组中删除，而访问控制列表不经常变化。

安全组工作原理

Windows 2000 Active Directory 支持安全组及分布组。安全组可以有与其相关联的安全权限，并且也可以作为邮件列表。分布组只用于邮件列表。它们没有安全功能。

创建一个新用户时，您可以将用户加入一个现存的安全组中，以完全定义该用户的权限和访问限制。对组更改一项权限会影响到该组中所有的用户。Windows 2000 带有几个预定义的安全组，而且创建您的新组也甚为容易。

安全组类型

Windows 2000 支持四种类型的安全组，其作用域不同：

- 本地域组最适合用于在要求公有访问权限的情况下授予对位于域中任何计算机上的资源的访问权，比如文件系统或打印机。用来保护资源的本地域组的优点在于：该本地域组的成员既可以来自同一个组内部也可以来自其外部。典型地，资源服务器在拥有和一个或多个主用户域的信任关系的域中，或者在称为帐户域的域中。（只有在本机模式域中，本地域组才可用于授予对任何计算机上的资源的访问权。在混合模式下，本地域组只能在域控制器上。）

- 全局组用于联合基于工作职责或商业角色共享一个公有访问配置文件的用户。典型地，单位对所有成员身份更改频繁的组使用全局组。这些组只能以拥有定义于和该全局组同一个域中的用户帐户作为成员。全局组可以嵌套，以允许覆盖安全需要或适应非常大的组结构的规模。对全局组授权的最方便的方法是：使得全局组成为一个资源组的成员，而该资源组则被授予了对一组相关项目资源的访问权限。

- 通用组用于更大的、多域的单位，在此需要对定义在多个域中的相似的帐户组授予权限。将全局组用作通用组的成员以减少由对通用组成员身份的更改导致的复制通信总流量就更好了。用户可以被添加到在其帐户域中的相应全局组中或从其中删除，少数几个全局组是通用组的直接成员。通过使其成为一个用于授予对资源的访问权限的本地域组的成员，通用组被轻而易举地授予了访问权。

  通用组只用于拥有全局编录的多域目录树或域目录林中。Windows 2000 域必须处于本机模式才能使用通用组。一个只有单个域的域模型不需要也不支持通用组。

- 计算机本地组是只针对一台计算机而在域中其他地方不被承认的安全组。如果一台成员服务器是一台文件服务器而且是多共享区中 100 GB 数据的主机，您可以为直接在这台计算机上执行的管理任务或为定义本地访问权限组而使用本地服务器组。

安全组的默认权限

对成员服务器与客户计算机来说，默认的 Windows 2000 访问控制权限提供了以下的安全级别：

- Everyone 组成员和 Users 组成员（普通用户）没有象在 Windows NT 4.0 中那样的广泛的读/写权限。这些用户对系统大多数部分拥有只读权限，而在其本身的配置文件文件夹中具有读/写权限。用户不能安装需要对系统目录进行修改的应用程序，也不能执行管理任务。
- Power Users 组的成员具有 Users 和 Power Users 在 Windows NT 4.0 中所拥有的全部访问权限。Power Users 除了对自身的配置文件文件夹以外，还对系统的其他部分拥有读/写权限。超级用户（”Power Users” 组中的成员）可以安装应用程序和执行许多管理任务。
- Administrators 组的成员拥有其在 Windows NT 4.0 中所拥有的同样级别的权限。

对配置为域控制器的服务器来说，默认 Windows 2000 安全组提供以下安全性：

- Everyone 和 Users 组的成员不具有象在 Windows NT 4.0 中那样的广泛的读/写权限。普通用户对系统大多数部分拥有只读权限，而在其本身的配置文件文件夹中具有读/写权限。然而，普通用户只能在网络上访问域控制器——用户不能象在 Windows NT 4.0 中那样交互式登录到域控制器。
- Account Operators、Server Operators、Print Operators 组的成员具有和在 Windows NT 4.0 中一样的访问权限。
- 正如 Windows NT 4.0 中一样，Administrators 组的成员可以完全控制系统。

实现安全组的先决条件

安全组是 Active Directory 的内置功能。不需要什么特殊的安装或先决条件。

实现安全组

要创建新用户并将其放入安全组中，请使用 MMC Active Directory 用户和计算机管理单元。有关创建新用户的详细信息，请参见 Windows 2000 Server “帮助”。

安全组的注意事项

设计潜在的安全组时，一种好的策略是：项目或资源的所有者根据所要求的权限定义其自身的本地组、并委派管理组成员身份的能力，这种能力自身也是组的一种权限。这种策略允许资源的所有者或项目领导者通过更新相应的组来管理访问。

一个安全组由部门或企业中具有相似角色的人组成。组通常以该角色命名，比如说 Account Operators、Administrators、Backup Operators 的 Windows 2000 内置组。自然属于相同项目或部门邮件列表上的人员可能也属于 Active Directory 中的相同安全组。Windows 2000 安全组有作为邮件列表的第二角色，因此这种相似性并非偶然。

使用符合项目组或责任的组是进行适当地授权的一种有效方法。一个部门的每个人都需要访问部门打印机。一个软件项目的工程师需要访问公用源目录。这些就是自然组。

注意，系统必须在登录时确定一个用户的所有通用组和全局组从属关系。如果用户是许多组的成员，当系统确定所有的组成员身份时，这会对性能造成一些影响。

一个用户可以登记的组的数目有一个上限。对于在一单个域中运行的单个用户来说，其通用组、全局组、以

及本地组的总数不能超过 1,000。然而，用户并不是被严格地限制在 1,000 个组中，因为这个限制是从单个域的角度施加于用户的。在多域模型中，可以假想一个用户是其帐户域中 500 个通用组和全局组的成员、一个资源域中 400 本地域组的成员、另一个资源域中 400 本地域组的成员、一台服务器中的 50 个本地组的成员、还是另一台服务器 100 个本地组中的成员。对于大多数实际用途来说，这个 1,000 个组的限度是非常大方的。

用嵌套组使得对大组管理组成员身份更为容易。（一个大组可能会有 5,000 个成员。）不要在您的 whole-company 组中分别列出每个雇员。whole-company 组如果被定义为包含您的部门组的组将会更易于管理。部门组可以被嵌套在 whole-company 组中。

如果您的 whole-company 组是一个通用组，这一点尤为重要。一个只有单个局域网 (LAN) 的单位可以使用通用组而不降低性能。然而，一个拥有广域网 (WAN) 的单位频繁更改通用组成员身份对站点间链路上的复制业务流量的影响。如果一个通用组的成员只包含其他的组，它就不会很频繁改变，而复制流量就基本上没有什么了。一个包含数千个单个用户的通用组很可能要求频繁地通过多条 WAN 链路更新，因为每一点更改都会复制到企业中所有的全局编录服务器上。将通用组定义为组的组减少了网络活动。

您可能会发现您的 Windows 2000 Server 不允许嵌套组。Windows 2000 Server 最初运行于混合模式，这意味着 Windows 2000 和 Windows NT 4.0 Servers 可以在同一个网络中互操作。混合模式对安全组有一些限制。当所有的服务器都已升级到了 Windows 2000 后，您可以转到本机模式。这是一个单向的转变，它启用诸如安全组嵌套的高级功能。

对一个特定的计算机来说，本地管理员安全组中的用户对这台计算机有完全的权限。当一台 Windows 2000 计算机加入一个域时，Domain Administrators 组被作为一个成员加入到本地管理员组当中。计算机的本机用户一般不需要是管理员组的成员。具有完全特权的管理员组必须用于本地管理活动，比如说更改系统配置。

您的网络安全部署规划说明您的安全组策略。请在部署规划中包括以下信息：

- 确定除了内置组以外您想要创建的通用组和全局组。
- 确定通用组、全局组、以及本地安全组（包括内置组）的成员身份要求。

安全组和复制冲突

如果在两个不同域控制器的管理员在不同站点同时更改成员身份，其中一项更改可能会丢失。这种情形只可能在您使得对组成员身份的更改快于系统能够复制它们的速度的情况下才能发生。当一个管理员向一个组添加成员或从其中删除成员时，整个组成员身份都会被复制，而不仅仅是复制更改的成员。如果两个管理员于两个不同域控制器上改变组成员身份，而且在第一个域控制器完成复制以前复制在第二个域控制器上发生了，则在 Active Directory 解决复制冲突后只有其中一项更改会保留下来。而另一项更改则丢失了。这样，一个用户可能会出乎意料地保留了对一项资源的访问权。

减少这种问题的一种方法是使用内置组。创建和特定站点相关的组，并将它加入将用于授权或拒绝对某资源的访问的父组中。然后，站点中的管理员可以更改这个与特定站点相关的组的成员身份，而不会丢失更改，只要这个组的成员身份在多个域控制器上的更新速度不比站点内的复制快就行。另外，如果将组成员身份更改的责任委派给每个站点上的一个管理员，所有的更改都会在一个域控制器作出，而复制冲突不会发生。

备注 在单个 Active Directory 站点内，随着域控制器数目增加，一项更改到达所有域控制器所要花费的时间也会增加，最长等待时间大约是复制器通知暂停时间间隔的三倍。通常，复制在单个站点内部会快速完成。两个或更多个 Active Directory 站点之间的复制通常耗时更长，并且是依赖于管理员所配置的复制日程安排的，也依赖于管理员是否配置了站间复制器通知。

要完全避免这种情形，请在单个域控制器上作所有的组成员身份更改。这将防止更改由于复制冲突而丢失。有关 Active Directory 的多主控冲突解决策略以及如何配置 Active Directory 以减少等待时间的详细信

息，请参见 *Microsoft Windows Server Resource Kit Distributed Systems Guide* 中的 “Active Directory Replication”。

建立信任关系

分布安全规划需要考虑被提议的域、域目录树、目录林、及非 Windows 2000 服务器结构。尽管 Windows 2000 自动建立默认信任关系，规划中仍要指出网络中哪些域是目录林的一部分，而哪些域需要明确信任。

对于同一目录林下的 Windows 2000 计算机，域之间的帐户身份验证由双向可传递的信任关系实现。新建域加入域目录树时，可传递的信任关系自动建立。信任关系由两域共享且定期更新的密钥定义。

如客户机与服务器在同一目录林下的不同域中，信任关系由 Kerberos v5 身份验证使用。

Kerberos 服务使用信任密钥创建信任域引荐票据。NTLM 身份验证也使用信任关系作为通行身份验证。通行身份验证使用信任链接密钥建立域之间的安全信道。在 Windows 2000 中，如果域在本机模式下，NTLM 身份验证也可支持可传递的信任。

域信任

域信任是一个有用的方法，允许用户从受信域访问信任域的服务。如果所有用户和服务都能在一个企业域中进行管理，就不需要信任关系。但是，创建不同的域有几个好处。域是一个区分域管理员责任范围的有用的方法。每个管理员只负责一个域内的用户和资源。域也是安全策略设置的范围，如帐户策略。大部分 Windows 2000 目录林中的信任关系是明确的双向可传递的信任，无需规划。对Windows NT 4.0 域或不同目录林的其它 Windows 2000 域的“外部”信任关系，需要在规划中涉及。

信任关系工作原理

所有域信任关系中只涉及两个域：信任域和受信域。域信任关系可分为以下几类：

- 单向
- 双向
- 可传递
- 不可传递

单向信任是指域 A 信任域 B 的单一信任关系。所有单向关系都不可传递。身份验证请求只能从信任域传递到受信域。这就意味着即使域 A 和域 B ，域 B 和域 C 有单向信任，域 A 和域 C 没有信任关系。

可与 Windows 2000 域建立单向信任的有:

- 不同目录林中的 Windows 2000
- Windows NT 4.0 域
- MIT Kerberos v5 领域

同一目录林的所有 Windows 2000 域由可传递的信任自动链接，通常不需要在同一目录林中的所有 Windows 2000 域之间创建单向信任。

一个 Windows 2000 目录林内的所有域信任都是双向可传递的。可传递的信任关系始终是双向的。这一关系

中的两个域互相信任。每次创建一个新域，在父域和新子域之间都会创建一个双向可传递的信任关系。这样，可传递的信任关系按其形成的方式通过域目录树向上流动，在域目录树中的所有域之间创建可传递的信任。

每次在目录林中创立一个新域目录树，在目录林根域和新建域（新域目录树的根）之间就会创建一个双向可传递的信任关系。可传递信任关系就这样在目录林中的所有域中流动。身份验证请求沿用这些信任路径，来自目录林中任何一个域的帐户都可在同一目录林中的任何其它域获得身份验证。

在同一域目录树的不同分支或同一目录林的不同目录树中的 Windows 2000 域之间可以明确（手动）创建可传递的信任。这种交叉结合的信任关系可以用来缩短大型、复杂的域目录树或目录林中的信任路径。在分布式安全规划中需要提供这些明确的信任。

不可传递信任限定在信任关系的两个域中，不会流动到目录林中的任何其它域。不可传递信任必须明确创建。不可传递信任的默认方式是单向的，但可以通过创建两个单向信任来创建一个双向关系。不同目录林中的域之间建立的所有信任关系都是不可传递的。

可传递信任只能在同一目录林的 Windows 2000 域之间存在。

总之，不可传递的域信任是下列各项之间唯一可能存在的信任关系：

- Windows 2000 域和 Windows NT 域。
- 一个目录林中的 Windows 2000 域和另一个目录林中的 Windows 2000 域。
- Windows 2000 域和 MIT Kerberos v5 领域。

实现信任的先决条件

除了要理解信任是域间的链接，信任没有其它特定的先决条件。要定义一个信任关系必须先建立至少两个域。

如何实现信任

要在同一目录林的域间设置明确的信任，打开 Active Directory 域和信任的 MMC 管理单元。右击一个域并打开属性列表。选择“信任”选项卡。用这个选项卡可以在同一目录林中的选定域和其它域之间添加、编辑或删除信任关系。

信任的注意事项

混合模式域（Windows NT 4.0 备份域控制器在网络升级期间与 Windows 2000 主域控制器临时结合）实现信任关系的方法与 Windows NT 4.0 工作站和服务器的 Windows NT 4.0 域一致。换句话说，Windows NT 4.0 工作站和服务器需要的所有信任关系混合模式域同样也需要。本机模式域（所有服务器都运行 Windows 2000）支持可传递的信任。

目录林中任何一个域的管理人员都有潜力取得所有权和修改 Active Directory 配置容器中的任何信息。这些改动可以得到并复制到目录林中所有域控制器。因此，对于加入目录林的任何域，都必须考虑那个域的管理员与其它域管理员同样受到信任。

对于域管理员没有得到完全或同等信任的域有两种处理办法。一种是给那个域设置一个明确的单项信任（或外部信任）。这样，登录到可疑域的用户就不能自动获得目录林其它部分的访问权。

要更精确地控制这种情况，考虑将可疑域的资源放入受信管理员所控制的域的一个单位（ Active Directory 文件夹）中。将单独的域一起删除。只能授予可疑域管理员以适当级别的计算机和本地组的控制权，而这些计算机和本地组都是管理员的域资源。

启用数据保护

信息安全策略不仅保护服务器和客户计算机上的数据，而且隐藏、保护穿越不安全网络的数据包。分布安全规划必须标识在计算机设备丢失或被盗的情况下，哪些信息必须予以保护。同样，规划中还应包括需要防止网络监探器进入的敏感或专用的网络通信类型。

针对企业网络用户，访问控制是保护敏感文件不受非授权访问的主要机制。访问控制在本章节前面部分已经讨论过。但是，计算机本身可携带而且可能被盗。要保护存储在这些计算机上的数据，访问控制是不够的。这是容易在旅行中被盗的膝上型电脑的一个特殊问题。为解决这一问题，Windows 2000 提供了加密文件系统 (EFS)。

为保证网络数据包的保密性，可以使用 Internet 协议安全（IPSec）为部分或所有服务器间的网络通信加密。IPSec 提供了在两台计算机之间设置已验证和加密的网络连接的功能。例如，可以配置电子邮件服务器要求与客户进行安全通信，从而防止数据包监探器读取客户机和服务器间的电子邮件消息。对于设计时没有考虑安全性的现有应用程序来说，IPSec 是保护数据的理想选择。

网络和拨号连接（远程访问）始终保护 Internet 或公共电话线上传输的网络数据。远程访问使用虚拟专用网络，该网络使用 IPSec 上的 PPTP 或 LT2P 隧道协议。

加密文件系统

Windows 2000 加密文件系统 (EFS) 让用户能够在本地计算机上给指定文件或文件夹加密，为本地存储的数据添加保护。EFS 自动为正在使用的文件加密并在文件存储时再次加密。除了为文件加密的用户和有 EFS 恢复证书的管理员，其他人都无法读取这些文件。由于加密机制已经内置在文件系统中，它的操作对用户是透明的而且很难攻击。

EFS 对保护可能被盗的计算机如膝上型电脑上的数据尤为有用。可在膝上型电脑上配置 EFS 以确保用户文档文件夹内的商业信息都已加密。即使有人想绕过 EFS 并试图使用低级磁盘工具读取信息，加密也能保护信息。

EFS 的主要目的在于保护本地 NTFS 文件系统磁盘上的用户文件。如果您离开这个模型（远程驱动器、多个用户、编辑已加密文件），还应了解许多例外情况和特殊条件。

EFS 工作原理

EFS 使用对每个文件都是唯一的对称加密密钥为文件加密。然后使用来自文件所有者 EFS 证书的公钥为加密密钥加密。由于文件所有者是唯一能够访问私钥的人，他也是唯一能为密钥、继而为文件解密的人。

使用管理员 EFS 文件恢复证书的公钥也能为初始加密密钥加密。这个证书的私钥可用来在紧急情况下恢复文件。建议单位建立恢复代理。

即使通过网络或计算机丢失造成文件被盗，如果不能先作为适当的用户登陆网络，文件也无法解密。既然无法读取文件，也就无法对其进行秘密修改。EFS 解决的是数据保密策略方面的问题。

实现 EFS 的先决条件

要实现 EFS，公钥基础结构必须到位，而且必须至少有一位管理员拥有 EFS 数据恢复证书，这样才能在文件原作者出现问题时为文件解密。文件作者必须有 EFS 证书。要加密的文件和文件夹必须存储在 Windows 2000 中的 NTFS 版本上。

如何实现 EFS

打开Windows 资源管理器，右击一个文件夹或文件。选择“ 属性 ”。在“ 常规 ”选项卡上，单击“ 高级 ”。然后选择“ 内容加密为安全数据 ”复选框。到清除复选框为止，该文件或选定文件夹中的所有文件内容现在都已加密。

关于对文件系统进行加密的最佳做法的详细信息，请参见 Windows 2000 Server “ 帮助 ”。还可参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide* 中的 "Encrypting File System"

EFS 的注意事项

只有 Windows 2000 使用的 NTFS 版本支持 EFS，EFS 不能与其它任何文件系统一起工作，包括以前的 NTFS 版本。

EFS 可用于在共享服务器上安全存储敏感数据，允许正常数据管理（备份）。服务器必须得到很好的保护，而且必须进行“ 受信委派 ”。给文件加密和解密时，EFS 服务“ 模拟 ” EFS 用户并代表他们进行其它网络连接。

EFS 使用数据恢复策略让得到授权的数据恢复代理为已加密文件解密。EFS 至少需要一个恢复代理。如果用户离开单位或将加密凭据丢失，恢复代理可以使用 EFS 恢复已加密文件。您需要规划部署 PKI 组件，为 EFS 数据恢复颁发一个或多个证书。这些证书需要脱机安全存储，防止损坏。EFS 可以为 EFS 用户和 EFS 恢复代理生成自己的证书。按照默认方式，EFS 向域管理员帐户颁发 EFS 恢复证书，使其作为域的恢复代理。对于没有加入域的单独计算机，EFS 给本地管理员用户帐户颁发 EFS 恢复证书作为该计算机的恢复代理。很多单位可能希望指定其它 EFS 恢复代理集中管理 EFS 恢复程序。例如，您可以为计算机组创建部门，为特定部门指定特定恢复代理帐户对 EFS 恢复进行管理。

您可以部署 Microsoft 证书服务，为 EFS 恢复代理和 EFS 用户颁发证书。如果有联机证书服务，EFS 使用证书服务生成 EFS 证书。

注意由于群集服务不支持共享存储上的重新分列点，如果文件服务器实际上是一个 Windows 群集，就不能使用 EFS。

网络安全部署规划应包含 EFS 策略和 EFS 恢复。EFS 策略可能包含下列信息。

- 膝上型电脑和其它计算机的文件系统策略。
- EFS 恢复代理。
- 推荐的 EFS 恢复步骤。
- 推荐的 EFS 恢复代理私钥管理和存档步骤。
- 支持 EFS 恢复证书所需的证书服务。

IP 安全

Windows 2000 与 Internet 协议安全 (IPSec) 相结合保护网络通信数据。IPSec 是允许两台计算机在非安全网络上进行安全的、已加密通信的一套协议。加密应用于 IP 网络层，这就是说它对大部分使用特定网络通信协议的应用程序都是透明的。IPSec 提供端到端的安全措施，意思是说 IP 数据包由发送计算机加密，在途中不可读取，只能由收件计算机解密。由于有特殊算法能够在连接两端生成相同的共享密钥，密钥不需要在网络上传递。

IPSec 工作原理

IPSec 有许多复杂的组件和选项值得详细研究，但在高层按以下方法运作：

1. 计算机 A 上的一个应用程序生成出站数据包通过网络发送到计算机 B 上。

2. 在 TCP/IP 内部，IPSec 驱动程序将出站数据包与 IPSec 筛选器比较，检查数据包是否需要安全措施。筛选器与 IPSec 安全规则内的筛选器操作相关联。许多 IPSec 安全规则在指派给计算机的同一个 IPSec 策略内。

3. 如果一个匹配的筛选器必须进行安全协商，计算机 A 使用一个被称之为“Internet密钥交换”(IKE)协议开始与计算机 B 安全协商，两台计算机根据安全规则中规定的身份验证方法交换身份标识凭据。身份验证方法可以是 Kerberos 身份验证、公钥证书或预共享的密钥值（与密码很相似）。 IKE 协商在两台计算机间建立两种协议，称为“安全关联”。一种（称为 “phase I IKE SA”）规定两台计算机如何互相信任并保护它们的协商。另一种是关于如何保护一种特殊类型应用程序通信的协议。该协议由规定每个通信方向的安全措施和密钥的两个 SA（称作 “phase II IPSecSAs”）组成。IKE 自动为每个 SA 创建并刷新一个共享密钥。密钥在两端独立创建，不通过网络传输。

4. 计算机 A 上的 IPSec 驱动程序在传出数据包上签名以保证其完整性，还可以使用协商中确认的方法有选择地为其加密以保证其机密性。它将安全可靠的数据包传输给计算机 B。

   备注：计算机 A 到计算机 B 网络路径上的防火墙、路由器和服务器不需要 IPSec。它们只是按通常方式通过数据包传递。

5. 如有必要，计算机 B 上的 IPSec 驱动程序检查数据包的完整性并为其内容解密。然后将数据包传输到接收应用程序上。

IPSec 提供了对付数据操纵、数据截取和重复攻击的安全措施。

IPSec 对数据机密性、数据完整性和认可策略都很重要。

实现 IPSec 的先决条件

网络中的计算机需要有 IPSec 安全策略， 其定义应适合网络安全策略和网络通信类型。同域的计算机可以按应用于组的 IP 安全策略分组。不同域的计算机可以由补充的 IPSec 安全策略支持安全网络通信。

如何实现 IPSec

可查看 MMC “组策略”管理单元中的默认 IP 安全策略。策略列在“Active Directory 的 IP 安全策略”或“IP 安全策略 (本地计算机)”下。

组策略对象
X 计算机配置
X Windows 设置
X 安全设置
X Active Directory 的 IP 安全策略

您还可以使用 MMC IP 安全策略管理单元查看 IPSec 策略。每个 IP 安全策略都包含决定何时以及如何保护通信的安全规则。右击一个策略，选择“属性”。“规则”选项卡列出策略规则。规则还可进一步分解成筛选器列表、筛选器操作和其它属性。

有关Internet 协议安全的详细信息，参见 Windows 2000 Server “帮助”。还可参见 *Microsoft® Windows®*

2000 Server Resource Kit TCP/IP Core Networking Guide 中的 "Internet Protocol Security"。

IPSec 的注意事项

IPSec 为传出和传入的数据包加密，代价是操作系统实施加密时增加了 CPU 的使用。在很多部署中，客户机和服务器都有相当多的可用 CPU 资源，因此IPSec 加密不会对性能产生明显影响。对于同时支持许多网络连接或向其他服务器传输大量数据的服务器而言，加密产生的额外成本是显著的。基于上述原因，在部署 IPSec 之前应使用模拟网络传输进行测试。如果使用第三方硬件或软件产品提供 IP 安全，测试也很重要。

Windows 2000 提供设备接口，允许使用智能网卡实现硬件加速 IPSec 每个数据包的加密过程。网卡供货商可能会提供几种版本的客户机和服务器卡，也可能不支持所有 IPSec安全措施的组合。研究每个卡的产品文档，确认它支持您部署时要采用的安全措施和连接数量。

您可以为每个域或部门定义 Internet 协议安全 (IPSec)。也可以在没有指派域 IPSec 策略的计算机上定义本地 IPSec 策略。您可以给下列各项配置 IPSec 策略:

- 指定 IPSec 客户间所要求的身份验证和机密性等级。
- 指定 IPSec 已知客户间允许通信的最低安全等级。
- 允许或阻止与 IPSec 未知客户的通信。
- 出于机密性考虑要求所有通信加密或允许明文通信。

考虑使用 IPSec 为下列应用程序提供安全措施。

- 单位内部网的对等通信，例如法律部或执行委员会通信。保护服务器上存储的敏感（秘密）信息的客户机-服务器通信对需要用户访问控制的文件共享点，考虑使用 IPSec 以保证这些数据通信时不会被其他网络用户看到。
- 远程访问(拨号或虚拟专用网络)通信。对使用 IPSec 和 L2TP 的虚拟专用网络需要设置允许 IPSec 计算机证书自动登记的组策略。有关 IPSec VPN 连接上的 L2TP 的详细信息，参见 Windows 2000 “帮助”。
- 安全的路由器-到-路由器 WAN 通信。

对于网络安全部署规划中的 IPSec 可考虑以下策略:

- 对使用 IPSec 通信的客户机和服务器进行标识。
- 标识客户身份验证是基于 Kerberos 信任还是数字证书。
- 描述每台计算机如何最初接收适当的 IPSec 策略并继续接收策略更新。
- 描述每个 IPSec 策略内部的安全规则。考虑如何需要证书服务通过数字证书支持客户身份验证。
- 描述为计算机注册 IPSec 证书的登记过程和策略。

设置统一安全策略

统一安全策略允许企业内部不同类别的计算机应用并且执行一致的安全设置，例如域控制器类别。做法很简单，创建一个部门，一个 Active Directory 内的文件夹，将合适的计算机帐户对象归入部门，然后在部门

内应用某一组策略对象。OU 计算机帐户代表的所有计算机就会自动一致执行组策略中指定的安全策略。

Windows 2000 带有可供选择的能自动应用于新建域和域控制器的默认组策略对象。也有可供选择的代表不同类型企业计算机安全等级的安全“模板”。模板可用于为一组计算机创建组策略或鉴定某个特定计算机的安全设置。

注意当前的讨论只限于组策略的“安全”设置。如果将组策略应用于一个部门，还应包括许多与安全无关的策略。关于这个机制的更大范围的讨论，参见 Windows 2000 “帮助”和本书中的“定义客户管理与配置标准”。

组策略

组策略对象包括主要应用于域或计算机（而不是用户）安全设置的大量安全权限配置文件。一个组策略对象可以应用到部门内的所有计算机。单个计算机启动时组策略得以应用，如果作出改动时没有重新启动计算机，组策略会得到定期刷新。

组策略工作原理

组策略对象与 Active Directory 用户中的域和部门（文件夹）以及计算机 MMC 管理单元相关联。组策略授予的权限应用到存储于该文件夹中的计算机上。使用 Active Directory 站点和服务管理单元还可将组策略应用到站点。

子文件夹从父文件夹继承组策略，子文件夹也可能依次有自己的组策略对象。指派给一个文件夹的组策略对象可能不止一个。关于组策略优先权和如何解决多个策略对象之间冲突的详细信息，参见 Windows 2000“帮助”。

组策略是安全组的补充。组策略可以让您将单一安全配置文件应用到多台计算机上。它加强了一致性并使易于管理。

组策略对象包含实现多种类型安全策略的权限和参数。

实现组策略的先决条件

组策略是 Windows 2000 Active Directory 的一个功能。编辑应用组策略对象前必须先在服务器上安装 Active Directory。

如何实现组策略

要察看部门示例及与其关联的组策略，打开 Active Directory 用户和计算机 MMC 管理单元，右击“域控制器”OU。打开属性页，单击“组策略”选项卡。选择“默认域控制器策略”，单击“编辑”。这样就打开了 MMC组策略管理单元。在这个模块中，指向“安全设置”。

组策略对象
X 计算机配置
X Windows 设置
X 安全设置

在“安全设置”下有九个安全策略设置子目录。本章后面将对这九个组进行简要描述。

实现组策略包括新建一个组策略对象（或修改现有对象），在对象内启动适当的设置，然后将组策略对象与包含域中计算机的部门链接。

组策略的注意事项

创建包括企业中承担类似角色的计算机的部门。用一个部门做域控制器。给应用程序服务器创建另一个部门。所有客户计算机可以放在另一个部门中。为实现安全设置一致性，将单一组策略对象应用到上述每个组。

建议将应用到用户和计算机的组策略对象数量减至最少。先做到这一点，因为每个计算机和用户组策略对象都必须在启动过程中下载到计算机，在用户登录时间下载到用户配置文件。多个组策略对象会增加计算机启动和用户登录时间。第二，应用多个组策略对象可能产生难以解决的策略冲突。

总之，组策略可由父站点传递到子站点、域、和部门。如果将一个特定组策略指派给高级的父站点，这个组策略会应用到父等级以下所有部门，包括每个容器中的用户和计算机对象。有关组策略设置继承的详细信息，参见本书的“ 定义客户管理与配置标准 ”。

作为适合不同类型组策略的安全设置模型，安全模板（详见本章后面部分）对您可能是有用的。

网络安全部署规划需要描述每个策略类别和子类别的重要策略选择。安全规划可以包括下列信息：

- 标识改变默认值的组策略设置。
- 描述所有改变组策略设置的相关问题。
- 描述特殊安全要求及如何配置组策略以满足特殊要求。

组策略安全设置

以下是本章前面提到的九种组策略安全功能。它们是位于组策略对象“ 安全设置 ”节点的容器。它们包括：

- 帐户策略
- 本地策略
- 事件日志
- 受限组
- 系统服务
- 注册表
- 文件系统
- 公钥策略
- Active Directory 中的网际协议安全策略

有些策略只应用于域的范围，也就是说，策略设置是在域范围内进行的。例如帐户策略一律应用于域内的所有用户帐户。不能为同一域内的不同部门定义不同帐户策略。

至于安全策略范围，帐户策略和公钥策略都具有域范围。所有其它策略范围都可在部门等级设定。

帐户策略

帐户策略是安全设置的第一个子类。包括下列内容：

密码策略 可以根据部门安全需要修改密码策略。例如，您可以设定最短密码长度和密码最长期限。为防止用户重复使用密码或简单改变密码，您也可以要求复杂的密码。

帐户锁定策略 可以强制锁定指定次数登录不成功的用户。您也可以设定帐户锁定的时间。

Kerberos 身份验证策略 您可以修改每个域的默认 Kerberos 设置。例如，您可以设置用户票据的最长使用时间。

您选择的策略影响用户要求的支持中心提供的支持和网络对抗安全破坏和攻击的能力。例如，设定限制性的帐户锁定策略增加了拒绝服务攻击的潜力，设定限制性的密码策略会导致无法登录网络的用户向支持中心的呼叫次数增加。

另外，指定限制性密码策略实际上会降低网络的安全性。例如，如果您要求密码长度在七个字符以上，大部分用户记起来会有困难。他们可能会将密码写下来，入侵者很容易找到。

本地计算机策略

安全设置的第二个子类是本地计算机策略。本地计算机策略包括下列内容：

审核策略 从系统范围内事件如用户登录，到某个用户试图读取某个文件， Windows 2000 可记录多种类型的安全事件。无论操作成功与否都可以记录。

用户权利指派 可以控制指派给本地计算机用户帐户和安全组的权利。您可以指定哪些用户和安全组有权执行一系列影响安全的任务。例如，您可以控制谁可以从网络访问计算机，谁可以在本地登录，或谁可以关闭系统。您可以指定谁有权在计算机上执行重要的管理任务，如备份和恢复文件与目录，取得文件和对象的所有权，以及从远端系统强制关机。

安全选项 您可以控制本地计算机的许多安全选项。例如，您可以指定策略强制登录时间已过的用户停止登录，停用 CTRL+ALT+DEL 登录(强制智能卡登录)，如无法审核可强制计算机暂停。

事件日志策略

使用事件日志策略可以在本地计算机控制应用程序、系统及安全事件日志的设置。例如，您可以指定日志文件的最大容量、记入日志的事件要保留多长时间以及日志保存方法。

受限组策略

您可以定义受限组策略来管理和实施内部成员身份或有特定权力和权限的用户定义组。受限组策略包括特定组的成员列表，他们的成员身份是作为安全策略的一部分集中定义的。受限组的实施自动设定计算机本地组成员身份使其与策略中定义的成员身份列表设置匹配。本地计算机管理员对组成员身份的变更由 Active Directory 中定义的受限组策略改写。

受限组可用来管理内置组的成员身份。内置组包括本地组，如管理员、电源使用者、打印操作员和服务器操作员，也包括全局组，如域管理员。您可以将您认为敏感或有特权的组及它们的成员身份信息加入受限组列表。这样您可以从策略上实现这些组的成员身份，不允许每台计算机上的本地改动。

系统服务策略

系统服务的机制有可能被入侵者利用，他们可以取代或利用服务作为访问计算机和网络资源的进入点。例如，入侵者可以设法利用正在运行的 Web 服务器的弱点访问计算机操作系统或文件。您可以将系统策略用于：

- 指定启动 Windows 2000 服务模式（手动或自动）或停用服务。

例如，您可以配置系统服务，防止运行不必要的服务。这样就为特殊服务器提供了最大程度的安全性，如域控制器、DNS 服务器、代理服务器、远程访问服务器和证书颁发机构服务器。

- 指定系统服务运行时授予的权力和权限。

  例如，您可以配置系统服务以最小的权力和权限操作，限制试图使用服务的入侵者可能造成的损害范围。

- 改进系统服务的安全审核水平。

  您可以指定记录失败和成功事件的事件类型。例如，如果审核已启用，您可以改进审核来监视运行服务中的不当操作。

注册策略

您可以使用注册策略配置安全设置，控制注册表项及其子项的安全审核。例如，为保证只有管理员才能更改特定注册信息，您可以使用注册策略授予管理员对注册表项及其子项的完全控制权，授予其他用户只读权限。您也可以使用注册策略防止用户查看注册部分。

如审核已启用，您可以使用注册策略审核用户在注册计算机时的活动。您可以指定哪些用户和用户事件记录到失败和成功事件详细信息中。

文件系统策略

您可以使用文件系统策略配置文件和文件夹安全措施，控制文件和文件夹的安全审核。例如，为保证只有管理员能更改系统文件和文件夹，您可以使用文件系统策略授予管理员对系统文件和文件夹的完全控制权，授予其他用户只读权限。您也可以使用文件系统策略防止某些特定用户查看文件和文件夹。

如审核已启用，您可以使用文件系统策略审核影响文件和文件夹的用户活动。您可以指定哪些用户和用户事件记录到失败和成功事件详细信息中。

公钥策略

使用这个安全设置的子部分，可以添加新的加密数据恢复代理并建立自动证书要求。您也可以管理受信证书颁发机构列表。

Active Directory 中的 IP 安全策略

这部分的策略告诉服务器如何回答 IPSec 通信请求。服务器可能要求安全通信、许可安全通信、或不使用 IPSec 通信。预定义策略的目的并不在于即时使用。它们出于测试目的提供性能示例。网络管理员需要仔细设计并给计算机指派自定义 IPSec 策略。

安全模板

Windows 2000 为您在网络环境设置中的使用提供了一套安全模板。“安全模板”是 Windows 2000 域控制器、服务器、或客户计算机上适合某一特定安全等级的安全设置配置文件。例如，hisecdc 模板包括适合高安全性域控制器的设置。

您可以把安全配置文件导入组策略对象并把它应用到一个等级的计算机上。把安全配置文件导入个人数据库用来检查和配置本地计算机的安全策略。

安全模板工作原理

安全模板提供标准安全设置作为安全策略的模型。帮助您解决计算机安全策略与策略不一致或未知的问题。导入组策略对象或安全配置和 MMC 分析管理单元前，安全模板处在非活动状态。

实现安全模板的先决条件

安全模板是 Windows 2000 的标准功能，使用它们没有先决条件。

如何实现安全模板

您可以在 MMC 安全模板管理单元编辑安全模板。

您可以使用 MMC 安全配置和分析管理单元导入导出模板，将模板与本地计算机的安全设置相比较。如果您愿意，可以使用 MMC 管理单元配置计算机使之与模板匹配。

要把安全模板导入组策略对象，打开MMC 组策略管理单元。右击“ 安全设置 ”容器，选择“ 导入策略 ”选项。这样就得到一些可以导入的安全模板。

有关使用安全模板和预定义模板的详细信息，参见 Windows 2000 Server “ 帮助 ”。

安全模板的注意事项

默认的 Windows 2000 全新安装权限使其安全性比以往版本的 Windows NT 明显增加。默认的全新安装安全机制由授予三个组的访问权限定义。用户、Power Users 和管理员。

根据默认方式，用户对非管理员系统应用有适当的访问控制策略；Power Users 与 Windows NT 4.0 用户后向兼容；管理员具有所有权限。这样，Windows 2000 系统的安全措施很大程度上取决于用户属于哪个组。

如果您的站点只运行兼容 Windows 2000 应用程序规范的应用程序，就有可能让所有用户都成为用户组成员，这样就可以实现最大访问控制安全性而不用牺牲应用程序功能。如果您的站点运行的应用程序与 Windows 2000 应用程序规范不兼容，只有 Power Users 有特权运行不兼容的应用程序。为使用户成功运行必须支持的应用程序，在考虑使用附加安全模板之前，必须先定义访问等级（用户、Power Users 或管理员）。

定义之后，安全模板可按下列方式使用：

基本 基本安全模板应用上文描述的 Windows 2000 默认访问控制设置。基本模板可用于已升级为 Windows 2000 的 Windows NT 计算机。这样升级计算机就符合只应用于全新安装计算机的新的 Windows 2000 默认安全设置。如果作了不想要的改动，基本模板也可以用来还原成默认设置。

兼容 为了运行与 Windows 2000 应用程序规范不符的应用程序，有些客户可能不希望让他们的用户成为 Power Users。因为Power Users 有附加的能力（例如创建共享的能力），这些能力超出了运行传统应用程序所需的访问控制设置范围。为满足客户要求，不让终端用户成为Power Users ，兼容模板用与大部分传统应用程序要求相符的方法“ 打开 ” 默认访问控制策略。例如，Microsoft® Office 97 SR1 作为 Power Users 或作为兼容配置下的用户成功运行。但 Office 97 不能作为全新安装用户成功运行。注意 Microsoft® Office 2000 作为全新安装用户成功运行因为它与 Windows 2000 应用程序规范兼容。计算机配置了兼容模板并不意味着安装了安全设置。

安全 安全模板修改设置（如密码策略、审核策略及注册值），这些设置不大会影响应用程序功能而更倾向于影响操作系统和网络协议的操作行为。安全模板的推荐值与已经定义的默认访问控制策略不同。安全模板不修改任何 ACL，但删除 Power Users 组的所有成员。

高安全 高安全模板通过安全模板中的几个参数增加了安全性。例如，如果安全模板启用 SMB 数据包签名，高安全模板会要求 SMB 数据包签名。安全模板对安装非签名驱动程序提出警告，高安全模板阻止非签名驱动程序安装。简而言之，高安全模板给许多操作参数配置成极限值，而不考虑性能、操作简易性或与使用第三方或更早 NTLM 版本的客户的连通性。与安全模板类似，高安全模板删除 Power Users 组的所有成员。

总之，使用安全模板必须考虑已安装的应用程序基础所要求的默认访问控制策略和其它网络系统的通信要求。由于模板修改操作系统设置，应用前必须先通过适当的质量保证测定。

部署安全应用程序

只建立分布式安全设置然后返回正常工作状态是不够的。安全的企业网络需要在设计时就考虑到安全功能的软件。不具备安全性的应用程序的原型应能够在网络上畅行无阻地传输密码。安全的环境需要安全的应用程序。

您在为企业评估软件时，要找设计有启用安全措施功能的应用程序。对已验证的网络连接寻找能与单一登录能力集成并具有在安全的计算机配置下正常运行能力的应用程序。不是管理员工具的软件不需要管理员特权。

Application Specification for Windows 2000 定义了应用程序要得到 Microsoft Windows 徽标的验证证书必须满足的技术要求。文档标识出安全应用程序必须支持的最小要求范围。

- 在安全的 Windows 2000 服务器上运行。
- 使用 Kerberos 身份验证进行单一登录以建立网络连接，。
- 用客户模拟支持一致的使用权限和安全组的 Windows 2000 访问控制机制。
- 应用程序服务使用服务帐户而不是本地系统（具有完全的系统特权）运行。

这些是最低限度的要求。部署设计巧妙的应用程序、避免缓冲区溢出或其它可能被入侵者利用的弱点，这一点也很重要。

一种方法是要求应用程序组件都要有数字签名。Microsoft® Authenticode™，通过 Microsoft® Internet 资源管理器，让用户从 Internet 下载软件组件前先识别发行人并验证无人篡改。

同时，经常提醒用户如果不熟悉电子邮件的来源或是不准备从发出地接收电子邮件，不要直接从电子邮件附件直接运行程序。

Authenticode 和软件签名

从 Internet 下载到用户计算机的软件可能包含未经授权的程序或病毒，这些病毒会造成破坏或给入侵者提供秘密网络访问途径。由于网络的互连性越来越高，恶意软件和病毒的威胁已经蔓延到 Intranet。

Authenticode 工作原理

为对付这种日益严重的威胁，Microsoft 开发了 Authenticode™ 技术，让开发者能够用标准 X.509 公钥证书给软件数字签名。用户可以验证发行商数字签名软件，由于发行商签了代码，用户也可以验证软件未经篡改。

您可以使用 Microsoft 证书服务给内部开发者颁发数字签名的证书。您的开发者可以先用签名证书给软件签名，然后再分发到 Intranet 上。为保护网络不受恶意软件和病毒侵犯，您还必须考虑建立策略防止用户从 Intranet 和 Internet 上下载和运行未签名软件。

对于在 Internet 上分发的软件，大部分用户倾向于信任那些用知名的商用证书颁发机构颁发的证书签名的软件。使用商用证书颁发机构也可以让您的单位无需为外部软件分发承担商用证书颁发机构的责任。因此，如果您在 Internet 上分发软件，需要考虑取得商用证书颁发机构的服务，给您的外部软件开发者颁发数字签名证书。

实现 Authenticode 屏蔽

您可按如下方式在 Internet 资源管理器中实现下载软件 Authenticode 屏蔽。在“工具”菜单，指向“ Internet 选项 ”， 单击 “ 安全设置 ” 选项卡。这个选项卡中更高等级的安全设置屏蔽软件组件以进行受信数字签名。

您可以通过组策略（本章前面部分描述过）控制这些 Internet 资源管理器安全设置。打开 MMC 组策略管理单元，指向 Internet 资源管理器容器。

组策略对象
X 计算机配置
X 管理模板
X Windows 组件
X Internet 资源管理器

Internet 资源管理器策略允许您锁定安全设置使用户无法更改，并要求所有下载组件都要有受信签名。

Authenticode 和软件签名的注意事项

部署规划的软件签名策略可以包含下列信息：

- 需要软件签名能力的内部和外部组。
- 用于内部分发的软件签名策略。
- 用于外部分发的软件签名策略。
- 支持软件签名策略所需的证书颁发机构部署和信任管理
- 用户成为软件签名者的登记流程和策略。
- 通知用户不要运行未签名或未受信组件。

安全电子邮件

当今企业中，包含敏感个人信息和专有商业信息的电子邮件消息经常在 Intranet 甚至 Internet 的非安全部分传递。间谍组织或电脑黑客很容易截取明文电子邮件消息。而且,不怀好意的人很容易在途中截取和修改电子邮件消息，或伪造发件人 IP 地址，发送错误邮件。

当今许多电子邮件安全解决方案，如 Microsoft 交换服务器都基于开放的 “ 安全/多用途 Internet 邮件扩展 (S/MIME) ” 标准。如果您想为商业伙伴、供货商和客户使用的第三方安全电子邮件应用程序提供交互操作能力，使用开放标准是很重要的。

安全电子邮件工作原理

基于 S/MIME 的安全电子邮件系统使用工业标准 X.509 数字证书和公钥技术保障发件人和收件人之间传递的电子邮件消息的安全。安全电子邮件系统提供下列有代表性的安全功能：

- 为提供数据完整性，发件人可以在电子邮件消息上进行数字签名。
- 收件人可以验证邮件发送者的身份并验证该邮件在途中未被篡改。
- 发件人不能否定签名邮件因为只有发件人拥有签名凭据。
- 发件人可以给电子邮件消息加密，以保证机密通信。
- 目标收件人可用专用凭据解密，其他人则无法解密和读取邮件。
- 管理员可在安全数据库中集中存储用户专用凭据。如用户专用凭据丢失或损坏，管理员可以检索解密所需专用凭据。

安全电子邮件的注意事项

要编写安全电子邮件策略，考虑在您的部署规划中包含下列信息：

- 要使用的安全电子邮件服务器和客户应用程序。
- 为保障电子邮件安全需要升级或迁移的电子邮件服务器和用户组。
- 在单位中使用安全电子邮件的常规策略。
- 要使用的加密技术，包括国际导出制约与限制。
- 支持安全电子邮件所需的证书服务。
- 安全电子邮件程序中用户登记流程和策略。
- 密钥恢复数据库备份能力和推荐的备份及恢复惯例。
- 密钥恢复能力和推荐的一般恢复惯例。

安全 Web 站点和通讯

Web 站点和浏览器已成为公开信息交换和部门 Intranet 和 Internet 协作的中心机制。但是，标准 Web 协议如“超文本传输协议 (HTTP)”提供的安全措施很有限。您可以配置大部分 WEB 服务器以提供基于用户姓名和密码的目录和文件等级安全措施。也可以由使用“公共网关接口 (CGI)”或“Active Server Pages (ASP)”的编程方法保障 Web 安全。但由于对 Web 服务器的攻击越来越频繁、复杂，这些保障 Web 安全的传统方法也变得越来越不能胜任。

您可以用 Internet 信息服务 (IIS) 与 Windows 2000 服务器为使用标准安全通信协议和标准 X.509 证书的 Web 站点和通信提供高水平的安全措施。您可为 Web 站点和通信提供下列安全措施：

- 用“安全套接字层 (SSL)”和“传输层安全 (TLS)”协议验证用户并建立加密通信的安全信道。
- 用“服务器控制加密 (SGC)”协议验证用户和建立加密财务事务处理安全信道。
- 将用户证书映射到网络用户帐户，按照用户拥有的受信证书颁发机构颁发的有效证书验证用户身份，控制用户使用 WEB 资源的权利和权限。

安全 Web 站点的注意事项

考虑在部署规划中包含以下信息：

- 升级或迁移至安全 Web 站点的 Web 站点和用户组。
- 用 SSL 或 TLS 保障客户机和 Web 服务器之间 Web 通信的策略。
- 控制用户使用 Web 站点资源的权力和权限的证书映射策略。
- 支持 Web 站点所需的证书颁发机构部署。
- 安全 Web 站点程序的登记流程和策略。

管理事务

安全规划中的一些策略会与 IT 部门员工有关。Windows 2000 支持管理权限的委派，允许特定人员拥有有限权力管理自己的组和文件。Windows 2000 也支持系统活动的审核日志，精确控制应记录哪些类型的事件以及记录的地点。

规划中应描述您计划如何保护域管理员帐户不受入侵者侵犯，这一点尤其重要。建议您建立域帐户策略，要求所有帐户使用长而复杂的密码以防被破解。这一点大家都理解，但您还是要在规划中清楚地说明。

太多人知道系统管理员密码，安全性就会被损害，这是显而易见的。域目录树的根域管理员也自动成为架构管理员组和企业管理员组成员。这是一个高特权帐户，入侵者可以从这里进行无限制的破坏。您在规划中要说明只有很少几个受信人员能够访问这个帐户。

只有执行需要管理员特权的任务时才能使用域管理员帐户。任何时候也不能登录这个帐户后无人管理。鼓励您的管理员人员使用另一个非特权帐户进行非管理活动（读取电子邮件，Web 浏览等）。

必须对用于域管理的服务器控制台进行控制，只有得到授权的人员才有权使用。在安全规划中要陈述这些要求，列出可以使用控制台的人员名单。管理员帐户使用者不得登录到由未得到同等信任的人进行管理的客户计算机上，这一点是显而易见的。其它客户计算机管理员有可能会把其它编码引入这台计算机，不知不觉地利用了管理员特权。

委派

Windows 2000 企业环境中委派管理员任务是实用和必需的。通常权限不仅委派给 IT 组成员，还要委派给人力资源人员和不同的经理，因为有些任务与其职责相关。委派分配了管理员工作量，而无需将大范围的特权授给每个助手。这是安全概念“ 最低特权原则 ”的体现，也就是说只授予执行任务所必需的权限。

通过不同方式，Windows 2000 允许您将对有限对象的规定程度的控制委派给组或个人。唯一的前提条件是适当的组元素（用户、组、组策略对象、文件、目录等）在委派前必须到位。

Windows 2000 支持通过不同功能实现的管理权委派，包括下文中列出的这些功能。（注意有些任务需要域管理员特权，不能委派。）

安全组、组策略和访问控制列表

这些功能本章前面部分已经描述过，它们构成了下文描述的功能机制。

内部安全组

Windows 2000 用已经委派给各组的特定权限预先定义了安全组。打开“ Active Directory 用户和计算机 ”MMC 管理单元。在“ 视图 ”菜单上选择“ 高级功能 ”。预定义的安全组在“ 内置 ”和“ 用户 ”文件夹中。

要直接委派对其中某一组的控制，打开组的属性列表，单击“ 安全 ”选项卡。将组经理添加到访问控制列表，选取适当的特权。

控制向导委派

打开“ Active Directory 站点和服务 ”MMC 管理单元。右击部门并选择“ 委派控制 ”。该向导设置用户组权限，管理特定站点和服务。例如新建远程访问帐户的权力。

委派管理向导

打开“ Active Directory 用户和计算机 ”MMC 管理单元。右击一部门并选择“ 委派控制 ”。该向导设置用户组权限，管理包括计算机和用户组的部门。例如委派新建用户帐户权。

委派组策略对象控制

通过组策略委派管理涉及下列三个任务，这三个任务可以按您的情况一起或单独执行。

- 管理站点、域或部门的组策略链接
- 创建组策略对象
- 编辑组策略对象

这些任务在本书中的“ 定义客户管理与配置标准 ”中有深入阐述。

审核

网络活动的审核和安全日志是重要的安全措施。Windows 2000 让您可以监视用于跟踪入侵者活动的多种事件。入侵者被识别后，日志文件记录可以作为法律证据。

审核工作原理

您可以规定一旦执行了特定操作或文件被访问，审核记录就会被写入安全日志。审核记录显示出执行的操作、执行的用户、操作的日期和时间。您可以审核成功或不成功操作，审核跟踪记录显示出谁在网络上执行了操作以及谁曾经试图执行不允许的操作。您可以在“ 事件查看器 ”中查看安全日志。

如果定期检查安全日志，就有可能在入侵者得手之前检测出某些类型的攻击，例如密码攻击。入侵者侵入后，安全日志可以帮助您确定入侵者是怎样进入的，他们都做了些什么。

审核日志是一个保障自身权利的策略。记录安全事件是一种检测入侵的方式。

实现审核功能的先决条件

不需要安装或购买什么。只须配置您的组策略设置以启用审核。您还必须在您想要跟踪的大范围或特定项目内启用审核。

如何实现审核功能

安全审核不能通过默认方式启用。只能用 MMC 组策略管理单元激活您所要求的审核类型。

组策略对象
X 计算机配置
X Windows 设置
X 本地策略
X 审核策略

可审核的事件类别包括：帐户登录事件、帐户管理、目录服务访问、登录事件、对象访问、策略更改、特权使用、过程跟踪和系统事件。注意审核策略以策略继承为准，在本地计算机设置的策略可能被为整个域设置的策略所覆盖。

一旦设置了审核策略，就可以通过对个别对象启用特定类型的审核信息实现精确控制。例如，要启用文件目录设置审核，右击 Windows 资源管理器中适当的文件夹。点向“ 属性 ”，单击“ 安全 ”选项卡。单击“ 高级 ”，然后选择“ 高级属性 ”对话框中的“ 审核 ”选项卡。即显示文件夹可用的审核事件列表。对于文件目录而言，可以选择将审核设置应用到文件目录中的文件和子目录中。

查看“ 事件查看器 ”中“ 安全日志 ”节点的审核信息。

关于审核安全事件的详细信息，参见 Windows 2000 “ 帮助 ”。

审核的注意事项

生成安全日志对服务器的磁盘空间有影响。您可以设置事件查看器改写超过“n”天的日志记录，或将服务器配置为在安全日志写满时停止运行。关于在安全日志写满时暂停计算机的详细信息，参见 Windows 2000 “ 帮助 ”。

注意这里描述的目录和文件审核功能需要 NTFS 文件系统。

监视防火墙内部的防火墙服务器和关键服务器，检测可疑活动。即使防火墙外部服务器被认为是非安全的，也要监视，因为它们提供了进入您企业的门户。

表 11.3 列出了需要审核的不同事件以及审核事件监视的特定安全威胁。

表 11.3 安全审核威胁检测策略

审核事件	检测到的威胁
登录/注销失败审核	随机密码破译
登录/注销成功审核	失窃密码侵入
对用户权力、用户和组管理、安全更改策略、重新启动、关机和系统事件的成功审核	滥用特权
文件访问和对象访问事件的成功和失败审核可疑用户或组对敏感文件读取/写入访问的文件管理器成功和失败审核	对敏感文件的不当访问
文件访问打印机和对象访问事件的成功和失败审核可疑用户	对打印机的不当访问

或组对打印机打印访问的文件管理器成功和失败审核	
程序文件（exe 和 dll 扩展名）的成功和失败写入访问审核过程跟踪的成功和失败审核运行可疑程序，检查安全日志看是否有修改程序文件或创建程序的非法企图只能在监视系统日志时运行	病毒爆发

分布式安全的规划任务列表

制定网络安全部署规划要完成表 11.4 列出的任务。

表 11.4 安全规划任务列表

任务	章节中的位置
标识您的网络适用的安全风险在规划中将这些风险制表并解释	安全风险
提供安全概念的背景材料和令读者了解规划的词汇表	安全概念
介绍并解释您规划中涉及风险的应对安全策略	分布式安全策略
确保所有对网络资源的访问需要使用域帐户进行身份验证	验证所有用户访问权限
确定哪部分用户群体需要使用强有力的身份验证进行交互式或远程访问登录	验证所有用户访问权限
定义域用户帐户的密码长度、更改间隔和复杂性要求，制定规划把这些要求传达到用户群体	验证所有用户访问权限
定义部门策略以消除任何网络上的明码电文密码传输，制定策略启动单一登录或保护密码传输	验证所有用户访问权限
如果强有力的身份验证能满足您的安全目标，确定针对智能卡登录部署公钥安全措施的规划,。	智能卡登录
描述启用用户远程访问策略	远程访问
制定远程访问通讯步骤规划，包括连接方法以及一般用户群体	远程访问
标识您的部门目前如何使用组并对组名以及如何使用组类别进行约定	应用访问控制
描述您准备为广泛的企业内资源安全访问采用的高等级安全组这些可能成为您的企业通用组。	应用访问控制
描述您的访问控制策略，特别说明如何通过一致的方法使用	应用访问控制

安全组。	
定义新建组的步骤和谁承担管理组员身份的责任	应用访问控制
确定哪个现存域属于目录林，哪个域使用外部信任关系。	建立信任关系
描述您的域、域目录树和目录林，并清晰地陈述它们之间的信任关系。	建立信任关系
定义标识和管理敏感或保密信息的策略以及您对保护敏感数据的要求。	启用数据保护
标识提供敏感数据的网络数据服务器，这些敏感数据可能需要网络数据保护以防止窃取。	启用数据保护
制定使用 IPSec 保护远程访问数据或访问敏感应用程序数据服务器的部署规划	启用数据保护
如使用 EFS，描述您的数据恢复策略，包括恢复代理在部门中的角色。	加密文件系统
如使用 EFS，描述您计划采取的完成数据恢复过程的步骤，验证这一过程对您的单位适用。	加密文件系统
如使用 IPSec，标识它在您网络中的使用方案，了解性能含义。	IP 安全
定义域范围内帐户策略，把这些策略和指导方针传达给用户群体。	设置统一的安全策略
确定针对网络上不同类别系统的本地安全策略要求，如桌面、文件和打印服务器、电子邮件服务器。定义适合每一类别的组策略安全设置。	设置统一的安全策略
在可以使用特定的安全模板管理安全设置处定义应用程序服务器，考虑通过组策略管理。	设置统一的安全策略
将适当的安全模板应用到由 Windows NT 4.0 升级而不是全新安装的系统。	安全模板
把安全模板作为描述您计划在不同类别计算机上实现的安全等级的方法。	安全模板
制定测试规划，验证您的公用商务应用程序在适当配置的安全系统下正确运行。	部署安全应用程序
定义能提供增强型安全功能以满足您部门安全目标的附加应用程序。	部署安全应用程序
说明您要求的下载代码安全等级。	Authenticode 和软件签名

部署实现所有用于公开分发的内部开发软件的代码签名内部程序。	Authenticode 和软件签名
说明您的管理员帐户和管理控制台安全策略。	管理事务
标识您打算为特定任务委派管理员进行控制的情况。	委派
标识您的审核策略，包括职员	审核

第 12 章 - 规划公钥基础结构

Microsoft® Windows® 2000 全面支持公钥基础结构 (PKI)。PKI 是指通过使用公钥密码对电子交易有关各方的合法性进行验证与鉴别的数字证书、证书颁发机构和其它注册机构组成的系统。

使用 Microsoft® 证书服务和其他证书服务，就可以设计满足您的公钥安全需要的 PKI。

本章内容

本章目标

本章将帮助您制订以下规划文档：

- 公钥证书需求
- 证书颁发和使用策略
- 证书颁发机构信任层次设计
- 证书使用周期策略和过程
- 证书吊销策略
- 证书备份和灾难恢复策略
- PKI 部署和实施时间表

资源工具包中的相关信息

- 有关基于密码系统的安全技术、PKI 和公钥技术的更多信息，请参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide* 中的“ Cryptography for Network and Information Security ”。
- 有关使用公钥技术的安全方案的更多信息，请参见 *Microsoft Windows 2000 Server Resource Kit Distributed Systems Guide* 中的“ Choosing Security Solutions That Use Public Key Technology ”。

公钥基础结构概述

公钥基础结构 (PKI) 是 Windows 2000 的一项基础技术，使多种与身份验证和加密相关的功能成为可能。因此，PKI 的规划必须在部署前期制订。

本节对 Windows 2000 中的 PKI 功能和工具做了简要说明。

PKI 工作原理

PKI 的基础是“ 证书 ”。证书是一个包含公钥和主题名称的数字签名声明。证书中可以有主题的多类名称，比如目录名、电子邮件名称和域名服务 (DNS) 名称。通过在证书上签名，证书颁发机构可以核实与证书上公钥相应的私钥为证书所指定的拥有人所有。

证书颁发机构，通常是第三方公司，负责向可信用户颁发包含公钥的证书。这种证书可以自由分发。公钥可以用于对数据加密，这种加密数据只有使用相应的私钥才能解密，私钥也被提供给用户。用户要保证私钥的安全，其他任何人都不能得到它。私钥还可以用于创建能由公钥进行确认的数字签名。

公钥密码系统的基本思想是使用两个相互关联的密钥。其中一个可以在双方间公开自由地传递或者在一个公用信息中心库中发布，而另一个则必须私有保密。公钥也有不同类型的算法，每个都有自己的特征。这意味着并不是总能用一种算法替代另一种算法。如果两种算法能够实现相同的功能，获得结果的具体机制也不尽相同。在公钥密码系统中，两个密钥要顺序使用。如果先使用公钥，再使用私钥，这是一个密钥交换操作。如果先使用私钥，再使用公钥，则是一个数字签名操作。

您可以在本企业内部创建自己的证书颁发机构，也可以使用第三方公司提供的商务证书服务。

PKI 处理信息时采用了同步识别和验证信息源的方式。这使得标识截取非常困难，从而避免了冒充访问和对数据的操纵。表 12.1 描述了企业中可以使用 PKI 的某些方式。

表 12.1 数字证书的主要应用程序

应用程序	用途
安全电子邮件	安全电子邮件客户使用证书确保电子邮件的完整性，并对电子邮件消息加密确保其机密性。
安全 Web 通讯	Web 服务器可以验证 Web 通信中的客户身份（使用客户证书），并提供加密 Web 通信（使用服务器证书）。
安全 Web 站点	Internet 信息服务 (IIS) Web 站点可以映射客户证书，验证用户身份以控制其对 Web 站点资源的权力和权限。
软件文件的数字签名	代码签名工具使用证书在软件文件上添加数字签名，对文件源提供保护，并保证数据的完整性。
本地网络智能卡身份验证	Kerberos 登录协议可以在网络用户登录网络时，使用证书和智能卡上的私钥验证他们的身份。
远程访问智能卡身份验证	运行路由和远程访问服务的服务器可以在网络用户登录网络时，使用证书和智能卡上的私钥验证他们的身份。
IPSec 身份验证	IPSec 可以使用证书为 IPSec 通信客户验证身份。
加密文件系统 (EFS) 恢复代理	恢复代理证书能够恢复其他用户加密的 EFS 文件。

实现 PKI 的先决条件

在企业中实现 PKI 是一个多阶段的复杂过程，需要进行规划并通过先导测试程序进行实验。Windows 2000 的一些功能如加密文件系统 (EFS) 和 IP 安全 (IPSec)，在网络管理员没有进行任何特殊准备的情况下就可以提供自身的证书。您可以马上部署这些功能。其他安全功能则可能需要不同层次的 CA。CA 的层次需要进行规划。

您所做出的第一个商业策略决定就涉及到选择 CA，包括内部的和外部的，这将是证书的来源。典型的 CA 层次采用三层体系结构。建议在您的规划中有一个根 CA，并且是脱机的。要实现证书策略，还需要第二层 CA。这个层次也需要脱机。第三层是颁发 CA。这个层次上可以是内部的也可以是外部的 CA。内部网络身份验证和数据完整性可由本地认证机构如 IT 部门处理。Internet 交易和软件签名可能需要第三方证书以建立公众可信性。

在选择 CA 时，需要适当考虑加密服务提供程序 (CSP)。CSP 是为 CA 提供加密服务的软件或硬件。如果

CSP 是基于软件的，它会在计算机上生成一个公钥和私钥，常称为密钥对。如果 CSP 基于硬件，比如智能卡 CSP，它可能会通知某个硬件产生密钥对。

Windows 环境下的标准 CSP 是 Microsoft Base 加密服务提供程序，提供 40 位密钥长度。Windows 2000 支持 40/56 位加密，并可以导出。要实现最高安全性（及更快的速度），可以考虑使用基于硬件的 CSP，可以从第三方供应商那里得到。

通常更高的安全性意味着更多的开销，这既包括硬件的费用，也包括花在加密上的 CPU 周期。更高的安全性从费用上来说并不总是高效的，但在需要时可以得到。对于极端层次的安全需求，不妨考虑让 CA 使用硬件 CSP，而让用户使用智能卡。

如何实现 PKI

公钥基础结构证书功能已经内建于 Windows 2000 和大多支持企业商业计算的软件中。如想了解 Windows 2000 PKI 的功能，请浏览以下章节：

建立本地证书颁发机构

您可以在 Windows 2000 服务器上创建本地 CA。在这里有几类 CA 可供选择。一类是企业 CA，能够为数字签名、电子邮件加密、Web 身份验证及智能卡 Windows 2000 域身份验证等目的颁发证书。企业 CA 基于用户或其他实体的申请颁发证书，并且需要 Active Directory™ 目录服务的支持。

独立 CA 也基于用户或其他实体的申请颁发证书，但与企业 CA 不同，它不需要使用 Active Directory。独立 CA 主要用于 Extranet 和 Internet。

CA 还可以履行各个层次的角色，比如根 CA、从属 CA 和颁发 CA。有关证书等级需要考虑的事项，请参见本章后面的“定义证书策略和证书颁发机构行为规则”。

要在基于 Windows 2000 的服务器上创建本地 CA，请

1. 单击“开始”，将鼠标指向“设置”，然后单击“控制面板”。
2. 双击“添加/删除程序”，然后单击“添加/删除 Windows 组件”。
3. 添加“证书服务”，安装企业根 CA。

有关如何安装本地证书颁发机构的更多信息，请参见 Windows 2000 Server 的“帮助”。

建立了本地 CA 之后，就可以使用 Microsoft 管理控制台 (MMC) 中的“证书颁发机构”管理单元，对 CA 进行监视和管理。

您也可以查看 PKI 证书。

要查看 PKI 证书的个人设置，请

1. 打开 Microsoft Internet Explorer。
2. 在“工具”菜单上，单击“Internet 选项”。
3. 在出现的对话框上，单击“内容”选项卡。该选项卡中部的按钮显示了当前证书、可信的证书颁发机构和可信的软件发行商等信息。

管理证书

要管理证书，请使用 MMC 的“ 证书 ”管理单元。注意，该管理单元有两种显示模式，即“ 逻辑证书存储区 ”模式和“ 证书目的 ”模式。单击“ 证书 ”节点（最上层节点），将其突出显示。在“ 查看 ”菜单上，单击“ 选项 ”。请您分别熟悉这两种不同的显示模式。

要在该管理单元上申请新证书，请在“ 证书目的 ”视图用右键单击适当节点，然后在“ 全部任务 ”菜单上，单击“ 申请新证书 ”。

使用证书服务 Web 页

Windows 2000 站点可以运行以后，就可以允许用户从内部证书颁发机构申请自己的证书了。您必须已经配置并运行了一个 CA，IIS 也必须经过配置并运行。请通过 http:// *computer_DNS_name*/certsrv/ 访问该登记 Web 页。

在组策略对象中设置公钥策略

一些 PKI 策略可以在组策略对象中设置，从而将其应用到域和部门作用域中的计算机。请打开适当组策略对象的 MMC “ 组策略 ”管理单元。PKI 项目位于“ 计算机配置 ”下面：

组_策略_对象
X 计算机配置
X Windows 设置
X 安全设置
X 公钥策略

证书信任列表和 CA 根证书是组策略对象的一部分，包含了组策略收件人可信任的 CA。在“ 公钥策略 ”下，分别是“ 企业信任 ” 容器和“ 可信的根证书颁发机构 ”容器。

建立公钥基础结构

Windows 2000 PKI 提供了基于标准的服务、技术和协议框架，让您能够使用公钥技术部署和管理强有力的信息安全系统。Windows 2000 支持分布式安全服务所需要的各种公钥安全功能。例如，Windows 2000 支持 EFS 所需的公钥密码系统运算，而不需要部署额外的基础结构或 CA。

但很多安全方案（比如安全电子邮件、智能卡身份验证和安全 Web 通讯）要求您设计、测试并部署额外的 PKI 组件，包括 CA、证书登记和证书续订，以支持此类应用程序。还有可能您想部署支持 EFS 用户、多个恢复代理或 IPSec 身份验证的证书服务，为那些没有运行或是不能使用 Kerberos 身份验证建立信任关系（在不可信 Windows 2000 域间，或与非 Windows 2000 域成员的计算机）的客户提供服务。此外，为了满足单位的特殊需要，您也可能想开发和部署自定义应用程序和证书服务。

图 12.1 显示了可用来在单位内设计、测试和部署 PKI 的基本过程。

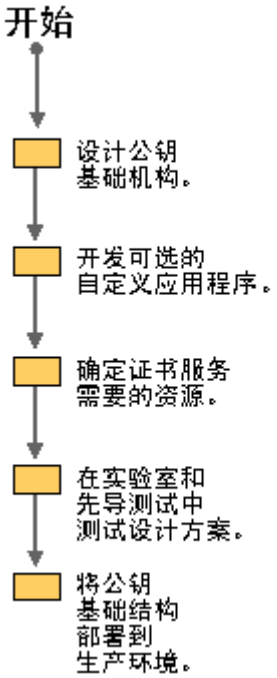


图 12.1 单位内设计 PKI 的流程图

可以使用 Microsoft 证书服务设计和部署 PKI。也可以使用第三方 Windows 2000 兼容 CA 建立部分或全部 PKI。不管使用哪种证书服务，建立 PKI 的基本过程都相同。但建立 PKI 的实际实现细节会因证书服务技术的不同而有所差异。有关 Windows 2000 公钥基础结构组件和功能的更多信息，请参见 *The Microsoft Windows 2000 Server Resource Kit Distributed Systems Guide* 中的“Choosing Security Solutions That Use Public Key Technology”。有关第三方证书服务组件和功能的更多信息，请与适当的证书服务提供商联系。

设计公钥基础结构

使用 Windows 2000，您可以设计满足广泛的公钥安全需要的 PKI。必须明确需要，以便设计和衡量基础结构来支持这些需要。

明确证书要求

在确定需要哪种 PKI 证书服务之前，必须明确要部署哪些使用数字证书的应用程序。还必须明确所有的证书使用情况，包括哪些用户、计算机和服务需要证书，以及打算颁发哪种证书。您可以部署 Microsoft 证书服务，也可以获取其他证书服务，支持对公钥的需求。请明确需要证书的用户、计算机和服务的类别，并为每个类别确定以下信息：

- 名称或描述
- 需要证书的原因
- 实体（用户、计算机或服务）数目
- 用户、计算机和服务的位置

在明确了组织中各商业部门的类别和位置之后，需要提供相应的证书服务。您所部署的证书服务决定于颁发

的证书类别、需要证书的实体数目和组所处的位置。例如，可以部署两个颁发 CA 为组织中的所有管理员组提供证书。但组织中的商业用户比管理员多，因此可能需要在各个职能部门分别部署颁发 CA，满足商业用户的需要。

有关使用数字证书的安全方案的更多信息，请参见 *Microsoft Windows 2000 Server Resource Kit Distributed Systems Guide* 中的“Choosing Security Solutions That Use Public Key Technology”。

对证书的基本安全要求

使用证书时，有几个基本因素会影响全局的安全。对打算使用的证书，请详细说明对以下因素的要求：

- **私钥的长度。**在典型部署中，用户证书使用 1,024 位密钥，而根 CA 使用 4,096 位密钥。
- **证书使用的加密算法。**建议使用默认算法。
- **证书和私钥的生存时间和续订周期。**证书的生存时间是由证书类型、安全要求、行业标准行为规则以及政府规章确定的。
- **私钥存储和管理的特殊要求。**例如，存储在智能卡上且不可导出的密钥。

Microsoft 证书服务颁发证书的标准设置可以满足一般的安全需要。但有可能您想为特定用户组的证书指定更强有力的安全设置。例如，对那些为非常宝贵的信息提供安全的证书，可以指定更长的私钥长度和更短的生存时间。还可以指定使用智能卡存储私钥，以提供额外的安全性。

确定要颁发的证书类型

明确打算颁发的证书类型。颁发的证书类型依赖于要部署的证书服务和为证书指定的安全要求。您可以颁发各种类型的证书，它们有多种用途、满足不同的安全要求。

对于企业 CA，可以颁发各种基于 Windows 2000 域证书模板和帐户特权的证书。您可以配置各企业 CA，让它们颁发一定类型的证书。表 12.2 列出了可用的不同证书模板类型及其用途。

表 12.2 证书模板及用途

证书模板名称	证书用途	颁发给
Administrator	代码签名、Microsoft 信任列表签名、EFS、安全电子邮件、客户身份验证	人
Certification authority	所有用途	计算机
ClientAuth	客户身份验证（已验证阶段）	人
CodeSigning	代码签名	人
CTLSigning	Microsoft 信任列表签名	人
Domain Controller	客户身份验证、服务器身份验证	计算机

EFS	加密文件系统	人
EFSRecovery	文件恢复	人
EnrollmentAgent	证书申请代理	人
IPSECIntermediateOffline	IP 安全	计算机
IPSECIntermediateOnline	IP 安全	计算机
MachineEnrollmentAgent	证书申请代理	计算机
Machine	客户身份验证、服务器身份验证	计算机
OfflineRouter	客户身份验证	计算机/路由器
SmartcardLogon	客户身份验证	人
SmartcardUser	客户身份验证、安全电子邮件	人
SubCA	所有用途	计算机
User	加密文件系统、安全电子邮件、客户身份验证	人
UserSignature	安全电子邮件、客户身份验证	人
WebServer	服务器身份验证	计算机
CEP Encryption	证书申请代理	路由器
Exchange Enrollment Agent (Offline Request)	证书申请代理	人
Exchange User	安全电子邮件、客户身份验证	人
Exchange User Signature	安全电子邮件、客户身份验证	人

对于独立 CA，可以在证书申请中指定证书的用途。还可以使用自定义策略模块指定颁发给独立 CA 的证书类型。有关为 Microsoft 证书服务开发自定义应用程序的更多信息，请参见 Web Resources 页的 Microsoft Platform SDK 链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

第三方证书服务所颁发的证书类型决定于各自的产品特性和功能。有关更多信息，请与证书服务提供商联系。

定义证书策略和证书颁发机构行为规则

您可以使用 Microsoft 证书服务或其他证书服务为单位创建 CA。在部署 CA 之前，请先定义证书策略和证书行为规则说明 (CPSs)。证书策略指定了证书可以用于哪些方面，及由 CA 认定的使用这些证书应承担的责任。证书行为规则说明指定了 CA 管理证书的行为规则。CPS 描述了证书策略的要求如何在 CA 组织的运行策略、系统体系结构、物理安全及计算环境中实现。例如，证书策略可能指定私钥不可导出，则 CPS 会

描述如何用部署的 PKI 将其实现。

证书策略

证书策略可以包括以下类型的信息：

- 如何向 CA 验证用户
- 法律问题如责任，这有可能在 CA 被泄密或用于不良目的时引发
- 证书用于何种目的
- 私钥管理的要求，比如要求存储在智能卡或其他硬件设备上
- 私钥可否导出
- 证书使用的要求，包括用户在私钥丢失或泄密时必须做什么
- 证书登记和续订的要求
- 证书生存时间
- 使用的加密算法
- 公钥和私钥对的最小长度

证书行为规则说明 (CPS)

证书颁发机构的 CPS 可以满足多种证书策略的要求。每个 CPS 都包含了 CA 本身的特定信息。但从属 CA 的 CPS 可参照父 CA 的 CPS 获取一般信息。CPS 可以包括以下各类信息：

- CA 的正标识（包括 CA 名、服务器名和 DNS 地址）
- CA 执行哪种证书策略，颁发哪种证书
- 颁发和续订证书的策略、程序及过程
- CA 证书所用的加密算法、CSP 和密钥长度
- CA 证书的生存时间
- CA 物理的、网络的及程序的安全性
- CA 颁发的各证书的生存时间
- 吊销证书的策略，包括证书吊销的条件如职员停止工作或滥用了安全特权
- 证书吊销列表 (CRL) 策略，包括 CRL 分发点和发布时间间隔
- 在 CA 证书到期之前续订的策略

定义证书颁发机构信任策略

部署 Windows 2000 PKI 之前，需要定义组织中使用的 CA 信任策略。

通过 Windows 2000，您可以使用分层 CA 信任链和证书信任列表建立 CA 信任关系。

证书颁发机构信任层次的优点

Windows 2000 PKI 有一个分层 CA 模型。CA 的层次结构提供了系统可扩展性、管理方便性以及与更多第三方产品的一致性等优点。

一般来说，在层次结构中会包含明确定义了父子关系的多个 CA。这一模型中，附属 CA（子）由（父）CA 颁发的证书确认，证书将一个 CA 公钥与该 CA 的身份绑定在一起。

层次结构顶端的 CA 称为根 CA。层次结构根以下的 CA 称为附属 CA。Windows 2000 中，如果您信任一个根 CA（将其证书放在可信的根证书颁发机构存储区），也因此会信任层次中的各个附属机构，除非它已被颁发 CA 吊销了证书，或者证书已经过期。因此，根 CA 是组织内一个非常重要的信任点，必须安全可靠。

这一模型的优点是验证证书只需要对少数根 CA 建立信任。同时，它还使证书颁发附属 CA 的数目更为灵活。部署多个附属 CA 有几方面的实际原因。包括：

用途。颁发证书可以出于很多用途（例如，安全电子邮件、网络身份验证等）。不同用途的颁发策略必须不同，分开处理是管理策略的基本依据。

组织划分。依赖于组织中各实体的角色，可能会有不同的证书颁发策略。同样，您可以创建多个附属 CA 分别管理这些策略。

地理划分。组织可能在多个物理站点拥有实体。这些站点间的网络连接可能要求多个附属 CA，以满足可用性。

多信任层次还提供了以下管理方面的优点：

- 可以灵活配置 CA 安全环境（密钥长度、物理保护、对网络攻击的保护等）。您可以调整 CA 环境，以在安全性和可用性之间提供平衡。例如，对于根 CA，可以使用特殊用途的加密硬件，把它放到加锁的保险库，并在脱机模式运行。但对于颁发 CA，同样的设置会很昂贵，并且难以使用，CA 的性能和效力也会下降。
- 可以为那些有高泄密风险的中级和颁发 CA 频繁续订密钥和证书，而不需要更改已建立的根信任关系。
- 可以关掉 CA 层次结构的一部分，而不影响已建立的根信任关系或层次其他部分。

另外，部署多个颁发 CA 还提供了以下优点：

- 为不同类别的用户和计算机及组织和地理划分分别提供证书策略。您可以为各不同类别、不同部门和不同站点设置不同的颁发 CA。
- 分散了证书负载、提供了冗余服务。您可以部署多个颁发 CA，以分布证书负载，满足站点、网络和服务器的要求。例如，站点间缓慢而不连续的网络链接要求在每个站点都有颁发 CA，以满足对证书服务性能和可用性的要求。如果需要，可以部署多个颁发 CA 来分散证书负载，满足所有站点和网络对连通性和负载的要求。还可以部署多个颁发 CA 提供复制服务。这样，一旦有 CA 发生故障，就可用其他颁发 CA 来提供不间断的服务。

证书信任列表的优点

证书信任列表是证书为单位内所信任的 CA 的自签名证书列表。证书信任列表让您可以控制证书颁发机构指

定范围之外的证书颁发机构颁发的证书的用途和有效期。不管什么时候创建证书信任列表，都需要用一个已被信任的证书颁发机构颁发的证书在证书信任列表上签名，完成对它的验证。

一个站点可以有多个证书信任列表。由于域或部门 (OU) 的证书使用情况可能不同，您可以创建证书信任列表反映这些不同，并为特定的组策略对象指派相应的证书信任列表。

在将组策略对象应用到站点、域或 OU 时，相应的计算机会继承策略。这些计算机会信任该证书信任列表中的 CA。还可以将根 CA 放入组策略。与使用组策略相比，证书信任列表更为方便，因为证书信任列表有失效期。

可以创建 Windows 2000 证书信任列表，获得以下优点：

- **从指定 CA 创建信任证书不需要对根 CA 有更广的信任。**例如，可以在 Extranet 上使用证书信任列表，建立对特定商业 CA 颁发证书的信任。通过将证书映射到 Active Directory 帐户，拥有可信商业 CA 证书的用户可被赋予访问 Extranet 受限资源的权限。
- **对可信 CA 证书的使用限制。**例如，一个 CA 颁发的证书可能对安全电子邮件、网络身份验证和签名软件代码有效。但您可以在 Extranet 上使用证书信任列表，将允许的使用限制到只对安全电子邮件有效。
- **对第三方证书和 CA 有效期的控制。**例如，一个商业伙伴的 CA 可以有五年的生存时间，而其颁发的证书有一年的生存时间。但您可以创建一个有六个月生存时间的证书信任列表，限制该商业伙伴 CA 证书在 Extranet 上受信任的时间。

证书颁发机构信任策略的其它注意事项

在定义 CA 信任策略时，请牢记以下方面：

- CA 信任层次的深度一般为四层（根 CA、中级 CA、颁发 CA 和颁发的证书）。
- 第三方 CA 可以构成全部或部分 CA 信任层次，但为了确保第三方 CA 能够提供期望的互操作性，请在实验室中测试计划方案。
- 一些第三方产品可能需要其他 CA 信任模型，而不具备与有根的 CA 层次的互操作性。Windows 2000 和大多商业 CA 都支持有根的 CA 层次。

定义证书颁发机构的安全要求

您应该定义对 CA 的安全要求。对 CA 的安全要求包括以下方面：

- 根 CA 使用基于硬件的 CSP
- 将根 CA 放在加锁的保险库中
- 让根 CA 和中级 CA（有时）脱机运行
- 保证中级 CA 和颁发 CA 处于安全数据中心
- 为根颁发机构和高层中级证书颁发机构提供更长的密钥

如果想从母公司将颁发机构委派到分支机构，可以使用脱机的中级 CA。然后为子公司提供一个附属 CA 以保证脱机。

决定 CA 的安全需要涉及到在实现和维护安全所需的成本、CA 受攻击的风险和 CA 泄密的代价之间找到平衡点。CA 受攻击的风险越高，CA 泄密的代价越大，表明保护 CA 安全的成本更高。通常应该为根 CA 提供最全面的保护，还要为中级 CA 提供比颁发 CA 更好的保护。

对根 CA 的保护也不一定花费昂贵，特别是对那些小公司来说。使用一个放在安全机柜中的脱机根 CA，或者使用存于保险库里的可移动媒体可能会非常合适。根 CA 计算机不应该安装网卡。

定义证书使用周期

证书的使用周期包括了以下事件：

- CA 被安装，证书颁发给 CA
- 证书由 CA 颁发
- 证书被吊销（如果必要）
- 证书被续订或过期
- CA 的证书被续订或过期

通常定义都会定义证书使用周期，以要求定期续订颁发的证书。颁发的证书会在生存时间结束时过期，可以在直到被吊销或过期或颁发 CA 不再可用的周期内续订。每个 CA 都可以在几个续订周期内颁发证书，直到该 CA 生存时间结束。此时，这个 CA 或者因为其密钥不能再用而退休，或者可以用一个新的密钥续订证书。

您应该定义满足商业目标和安全要求的证书使用周期。选择使用周期依赖于各种考虑，比如：

CA 和颁发的证书密钥长度。一般来说，较长的密钥支持较长的证书生存时间和密钥生存时间。

CSP 提供的安全性。一般基于硬件的 CSP 比基于软件的 CSP 更难泄密，因此支持更长的证书和密钥生存时间。

用于加密运算的技术能力。一些加密技术提供了更强的安全性，也支持更强的加密算法。您也可以使用 FORTEZZA Crypto 加密卡来提供比标准智能卡更强的安全性。通常，难于击破的加密技术会支持更长的证书生存时间。

CA 及其私钥的安全性。一般，CA 及其私钥的物理安全性越高，CA 的生存时间越长。

颁发的证书及其私钥的安全性。例如，智能卡上的私钥比本地硬盘文件中的私钥更加安全，因为智能卡不能被强制导出私钥。

攻击风险。受攻击的风险依赖于网络有多安全，CA 信任链保护的网络资源有多少价值，以及攻击本身的成本有多高。

对证书用户的信任程度。通常，较低的信任程度要求更短的使用周期和更短的密钥生存时间。例如，可以给临时用户比正常商业用户更低的信任，因此给他们颁发的证书生存时间更短；还可以对临时用户的证书续订要求更严格的控制。

愿意为证书续订和 CA 续订付出的管理努力。例如，为了降低续订 CA 要求的管理努力，您可以为证书信任层次指定更长、更安全的生存时间。

请仔细考虑您想让 CA、颁发的证书及密钥在多长时间内可信。证书和私钥的有效期越长，安全泄密的风险

和可能也就越大。

应该定义能够平衡商业目标以及安全需要的证书使用周期。不切实际的过短使用周期会导致维护这些使用周期需要作出过多的管理努力。不切实际的过长使用周期则会增大安全泄密的风险。

在使用 Microsoft CSP 续订证书时，还可以续订证书的密钥对。通常，密钥对使用的时间越长，泄密的风险也就越大。您应该设定密钥最大允许生存时间，并在期限到达之前续订有新密钥的证书。

定义了使用周期之后，通过在与原先指定不同的阶段续订 CA、证书或密钥，就可以对它更改。例如，如果后来认为与原先估计相比，根 CA 的生存时间把 CA 置于更大的泄密风险，您就可以在必要时续订该 CA 链，调整其使用周期，降低风险。

定义证书登记和续订程序

定义用于组织的证书登记和续订程序。Microsoft 证书服务支持以下证书登记和续订方法：

- 使用证书申请向导的交互式证书申请（只对 Windows 2000 用户、计算机和服务）。
- 使用自动证书申请向导的自动证书申请（只对 Windows 2000 计算机证书）。
- 使用 Microsoft 证书服务 Web 页的交互式证书申请（对大多 Web 浏览器客户）。
- 使用智能卡登记站的智能卡登记。
- 使用 Microsoft 登记控件的自定义证书登记和续订应用程序。

对证书登记和续订过程的选择决定于作为服务对象的用户和计算机。只有对 Windows 2000 客户，才可以使用证书登记向导。但对大多拥有 Web 浏览器的客户，都可以使用基于 Web 的登记和续订服务。

可以原样使用 Microsoft 证书服务 Web 页，也可以自定义这些页面。例如，可以限制用户选项，或者提供指向联机用户帮助和用户支持信息的其他链接。

定义证书吊销策略

单位的证书吊销策略包括吊销证书的策略和证书吊销列表 (CRL) 策略。

吊销证书的策略

证书的策略指明了需要吊销证书的情况。例如，可以指定在职员工作终止或转到其他部门时，证书必须吊销。或者在用户滥用其安全特权或私钥泄密（比如丢失智能卡）时证书必须吊销。对于计算机证书，可以指定在计算机被替换或从服务中永久删除或者密钥泄密时证书必须吊销。

证书吊销列表的策略

CRL 策略指定了在哪些地方分发 CRL，以及 CRL 发布的日程。例如，可以指定特定 CRL 将要分发到普通公用文件夹、Web 页及 Active Directory。还可以指定特定 CRL 会在每天发布，而不是默认的每周发布。

定义维护策略

为 CA 定义维护和灾难恢复策略。维护和灾难恢复策略包括以下内容：

- 要为 CA 执行的备份类型
- 进行 CA 备份的日程安排
- CA 恢复策略
- EFS 恢复代理策略
- 安全邮件恢复策略

制定恢复计划

可以制定恢复计划，这样在证书服务失败或 CA 泄密时可以帮助恢复 CA。为了确保恢复计划能够如愿运行，请测试这些计划并培训管理人员使用这些计划。

恢复计划包括以下内容：

- 管理员遵循的恢复程序和检查列表
- 恢复工具包或工具包的路径
- 应急计划

有关在 Windows 2000 中备份和故障恢复的更多信息，请参见本书的“确定 Windows 2000 存储管理策略”。

出故障的证书颁发机构

CA 可能会因各种原因发生故障，比如服务器硬盘故障、网卡故障或是服务器主板故障。一些故障通过定位并纠正 CA 服务器的问题是可以快速解决的。例如，可以将一块出故障的网卡或是主板替换，然后重新启动计算机，恢复证书服务。

如果硬盘发生故障，可以替换硬盘并从最新备份组中恢复服务器和 CA。如果 CA 被损坏或是破坏，可以从服务器最新备份组中恢复该 CA。

如必须替换服务器，请使用与故障 CA 服务器相同的网络名称和 IP 地址配置新服务器。然后用“Windows 2000 备份”或“证书颁发机构还原”向导从最新备份组恢复该 CA。

泄密的证书颁发机构

如果一个 CA 已经泄密，则必须吊销该 CA 的证书。吊销 CA 的证书也就是使 CA 及其附属 CA 无效，同时也使该 CA 及其附属 CA 颁发的证书无效。如果发现了泄密的 CA，请尽快执行以下行动：

- 吊销该泄密 CA 的证书。如果该 CA 已被续订，则只有该 CA 的全部证书都被泄密时，才吊销全部证书。
- 发布包含该吊销 CA 证书的新 CRL。注意，客户应用程序会储存 CRL 直到它过期，所以在旧的 CRL 过期之前，您不会看到新发布的 CRL。
- 从可信的根证书颁发机构存储区和 CTL 中删除泄密的 CA 证书。
- 通知受泄密影响的所有用户和管理员，告诉他们该 CA 颁发的证书已被吊销。
- 修复引起泄密的任何问题。

为了恢复 CA 的层次，必须部署新的 CA，或是续订 CA 证书并生成新密钥，替换已破坏的层次结构。然后，

必须为用户、计算机和服务重新颁发适当的证书。根据吊销在层次结构中的位置不同，可能需要一个全新的 CA 层次，或者只需要更换一部分。

开发可选的自定义应用程序

您可以选择部署各种各样带有 Windows 2000 PKI 标准组件和功能的公钥安全方案。但也可以使用 Microsoft CryptoAPI 开发自定义应用程序。

使用 CryptoAPI，可以开发自定义策略模块和自定义退出模块，并与现有的数据库和第三方目录服务集成证书服务。例如，可以开发一个应用程序，允许从现有数据库或第三方目录服务中的用户信息申请证书。

还可以开发一个使用特殊类型证书的自定义应用程序。例如，可以开发一个应用程序，能够创建电子文档的数字微缩图然后存入一个时间和日期戳记证书。可以将这些戳记证书放在文档注册表数据库中维护，以保护原文档内容的完整性。将文档与注册表数据库中的数字微缩图进行比较，就能够识别文档被注册后的任何篡改或修改。您可以使用这样的文档注册表为制造的产品提供联机质量保证审核跟踪，以确保电子测试和证书文档的完整性。

此外，您可以开发一个带有 Active Server Page 的自定义证书登记和续订应用程序。例如，可以修改标准 Microsoft 证书服务 Web 页，添加或删除一些功能。还可以开发与第三方服务或开发的其他应用程序集成的自定义 Web 页。

有关为 Microsoft 证书服务开发自定义应用程序的更多信息，请参见 Web Resources 页的 Microsoft Platform SDK 链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

执行资源规划

应该估计一下支持打算在单位中部署的证书服务需要多少网络、计算和设备资源。需要的资源量会因单位的规模、要部署的 PKI 的层次和作用域的不同而相应变化。

在估计资源时，请同时考虑支持短期及单位长期成长需要的资源。

部署需要的网络和计算资源包括：

- 运行证书服务和自定义应用程序的服务器计算机
- 加密硬件，如加密加速板
- 证书数据库和自定义应用程序的硬盘存储
- CA 和自定义应用程序备份需要的存储资源
- 灾难恢复资源，如恢复工具包和热备份替换服务器

证书服务的性能会因以下因素而有所差异：

- **用于证书签署的 CA 密钥长度。**密钥越长，证书签署需要的处理能力越强，需要时间越多。需要注意的是，每个证书签署操作只在颁发时执行一次（在服务器上），而验证操作在证书的生存时间内要执行多次（在客户或其他服务器上，因协议而异）。注意证书签署要比验证花费更高。
- **用于确认证书申请的证书颁发机构策略模块的逻辑复杂性。**策略逻辑越复杂，处理和颁发证书需要的时间越长。多数人会发现 Windows 2000 企业和独立策略模块已经足够。如果想开发自定义策略模块，则

需要考虑策略模块和退出模块的复杂性造成的成本。

- **自定义应用程序的性能影响。**自定义应用程序会影响证书应用程序的整体性能。例如，一个使用标准公共网关接口 (CGI) 脚本的证书登记应用程序可能会极大地延迟登记过程。

证书数据库要求的硬盘能力依赖于以下因素：

- **有多少证书要由 CA 颁发。**计划 CA 的生存周期内要颁发多少证书。需要颁发大量证书或有较长的生存时间的 CA 会需要更大的证书数据库。
- **每个证书的大小。**证书数据库包括了证书的所有信息，包括公钥。对于有较长公钥的证书和包含附加特殊信息的证书，每个占用的磁盘空间会更多。

一些大证书数据库可能会有几个 GB 或更大。但较小的证书数据库通常不会超过几百兆。您应该在实验室中测量典型的证书数据库大小，然后依据各个 CA 在其生存时间内计划要颁发的证书数目来推断未来的数据库大小。

部署公钥基础结构

在用先导测试程序对公钥设计和部署策略进行了验证和优化之后，您就可以将 PKI 部署到生产环境中了。下面的列表显示了一个基本生产应用过程，可以用它来部署 PKI。

部署 PKI 包括以下活动：

- 分阶段计划生产实施
- 为生产用户提供培训和支持
- 安装 CA
- 安装和配置支持系统或应用程序
- 配置要颁发的证书
- 配置证书吊销列表的发布
- 配置公钥组策略
- 配置证书续订和登记
- 为用户、计算机和证书颁发机构颁发证书

分阶段计划生产应用

对于大型企业部署，请分阶段计划公钥生产应用过程。如果必要，可以分阶段应用基础结构的不同部分以支持安全目标和商业需要。

例如，可以 EFS 和 IPSec 功能作为起点，因为得到这些功能的安全优点不必建立整个 CA 层次。下一步，可以优先考虑安全电子邮件和智能卡身份验证。可以选择将安全邮件基础结构的实施安排在智能卡基础机构实施之前，也可以安排组或站点的安全邮件和其他组或站点的智能卡基础结构同步进行。

为了实施安全邮件的 PKI，可以为应用各阶段安排以下活动：

- 在单位每个目录树的父域中安装安全邮件根 CA（根 CA 用于验证该域或其子域中的中级 CA）。
- 安装并配置安全邮件系统和服务（如有必要）。
- 在域或子域中，为每个商业部门安装安全邮件中级 CA（每个商业部门为其用户组验证和安装颁发 CA）。
- 如果必要，在域或子域中为每个站点的用户组安装并配置颁发 CA（由商业部门验证）和证书登记服务。

为了实施智能卡 PKI，可以为应用各阶段安排以下活动：

- 在单位每个目录树的父域中安装智能卡根 CA（根 CA 用于验证该域或其子域中的中级 CA）。
- 为用户和智能卡管理员安装并配置智能卡阅读器。
- 在域或子域中，为每个商业部门安装智能卡中级 CA（每个商业部门为其用户组验证和安装颁发 CA）。
- 如有必要，在域或子域中为每个站点的用户组安装并配置颁发 CA（由商业部门验证）和智能卡登记站。

此外，您可以安排实施其它部分的 PKI，以支持其它的公钥安全功能，如安全 Web 通讯和安全 Web 站点、软件代码签名、IPSec 身份验证及 EFS 用户和恢复操作。

安装证书颁发机构

要提供单位要求的证书服务，必须安装必要的 CA 层次。首先安装根 CA，然后是层次中的各个中级 CA。例如，要创建一个三层 CA 结构和信任链，可以按下述顺序在服务器计算机上安装 CA。

1. 根 CA
2. 中级 CA
3. 颁发 CA

根 CA 证书是自签名的。各中级 CA 由层次中的父 CA 验证（为其颁发证书）。在三层证书结构的例子中，各中级 CA 由根 CA 验证，而各颁发 CA 由中级 CA 验证。

备注 一个中级 CA 有可能由另一个中级 CA 验证，从而形成一个更深的层次结构。

您可以安装企业 CA、独立 CA 或者第三方 CA，以创建需要的信任链。要创建 Windows 2000 Server CA，请使用“控制面板”中的“添加/删除软件向导”向各 CA 服务器添加 Microsoft 证书服务。

在安装 Windows 2000 Server 附属 CA 时，可以从一个联机 CA 中申请附属 CA 证书，也可以将证书申请保存到申请文件，然后脱机申请证书。如果选择了脱机 CA 证书申请，则 CA 不被验证。证书颁发机构的的父 CA 为其颁发了证书之后，必须使用“证书颁发机构” MMC 管理单元手动将该 CA 的证书导入，完成 CA 的安装。还可以使用同一管理单元导入第三方父 CA 颁发的附属 CA 证书。

安装和配置支持系统和应用程序

必须安装 PKI 要求的所有系统和应用程序。支持系统和应用程序可能包括：

- 本地计算机上的智能卡阅读器
- 安全电子邮件和密钥管理系统

- 自定义策略和退出模块
- 自定义证书登记和续订应用程序
- 第三方 PKI 和证书服务
- 用于服务器上加速和密钥存储的基于硬件的加密卡

配置待颁发的证书

作为默认，Windows 2000 企业 CA 已安装完毕，可以颁发各种类证书。您可以使用“ 证书颁发机构 ” MMC 管理单元来修改默认配置，指定各个 CA 要颁发的证书类型。也可以删除不想让 CA 颁发的默认证书类型，或添加更多要 CA 颁发的证书类型。

配置示例

可以将 CA 配置成支持多种安全功能或是只支持一种安全功能。以下是配置 CA 的一些方法：

- 对于根 CA 或中级 CA，可以配置成只能颁发附属证书颁发机构证书。
- 对于一个支持 Web 通讯服务的颁发 CA，可以配置成只能颁发身份验证会话、计算机和 Web 服务器的证书。
- 对于支持一般商业用户的颁发 CA，可以配置成只能颁发用户证书。同样，可以将支持管理员的 CA 配置成只能颁发管理员证书。
- 对于支持智能卡登记的颁发 CA，可以配置成只能颁发智能卡登录和智能卡用户证书。

证书模板的安全访问控制列表

证书类型的申请权限由各证书模板的安全访问控制列表控制。只有在用户、计算机或服务的登记权限已被选入证书模板安全访问控制列表时，企业 CA 才会批准其证书申请。证书模板的安全访问控制列表已事先配置，允许各种默认用户帐户和安全组登记证书类型。

您可以使用“ Active Directory 站点和服务 ” MMC 管理单元来修改各个证书模板的安全访问控制列表。

要修改各证书模板安全访问控制列表，请

1. 在“ 查看 ” 菜单上，单击“ 显示服务节点 ” 。
2. 展开“ 服务 ” 节点和“ 公钥服务和证书模板 ” 容器。
3. 在详细资料窗格中选择证书模板，单击其属性页的“ 安全 ” 选项卡。该选项卡显示了可以访问这些模板的组以及各组的权限。

例如作为默认，只有“ 域管理员 ” 组的成员可以申请并获得登记代理证书。但为了指定只有安全部门中的特定成员才可以申请并获得登记代理证书，您可以更改登记代理证书模板的安全访问控制列表。在访问控制列表中删除域管理，添加适当的用户帐户或者安全组。

对于 Windows 2000 独立 CA，证书类型的信息必须包括在证书申请中，因为独立 CA 不使用证书模板。可以使用带有自定义策略模块和自定义证书申请应用程序的独立 CA，来控制颁发的证书类型。

配置证书吊销列表发布

作为默认，企业 CA 每周将 CRL 发布到 Active Directory。同样，独立 CA 和企业 CA 每周将 CRL 发布到 CA 服务器上的一个目录。您可以使用“证书颁发机构” MMC 管理单元来修改 CRL 的分发点。还可以使用“证书颁发机构”管理单元来交互地发布新 CRL，或者更改发布日程。

配置公钥组策略

您可以使用“组策略” MMC 管理单元来为站点、域和部门配置公钥组策略。可以配置公钥策略的以下可选类别：

EFS 恢复代理。

作为默认，安装在域中的第一个域控制器的本地管理员用户帐户是域的 EFS 恢复帐户。通过将适当备用代理的 EFS 恢复代理证书导入策略，就可以为 EFS 指定备用加密数据恢复代理。因此，必须首先为本地计算机上想用作备用恢复代理的用户帐户颁发 EFS 恢复代理证书。

自动证书登记

您可以为计算机证书指定自动登记和续订。在配置了自动登记之后，指定的证书类别会颁发给公钥组策略作用域中的所有计算机。自动登记颁发的计算机证书要从颁发 CA 续订。如果没有企业 CA 联机处理证书申请，自动登记不会有效。

对于使用 L2TP IPSec 的虚拟专用网络 (VPN)，请记住要设置组策略，以允许 IPSec 证书自动登记。表 12.2 中，颁发给计算机帐户中计算机的每个 RSA 公开公钥密码系统 (RSA) 签名证书都可以用于 IPSec。有关 IPSec VPN 连接上的 L2TP 证书的更多信息，请参见 Windows 2000 Server“帮助”。

根证书信任关系

在安装了企业根 CA 后，该 CA 的证书会被添加到域的可信的根证书颁发机构。您还可以交互地将其它根 CA 证书添加到“组策略” MMC 管理单元中的“可信的根证书颁发机构”容器。所添加的根 CA 证书即成为组策略中的可信的根 CA。如果想使用独立 CA 或第三方 CA 作为证书层次中的根 CA，则需要将该 CA 的证书添加到“组策略”中“可信的根证书颁发机构”容器。

证书信任列表

您可以创建证书信任列表来建立对特定 CA 的信任并限制这些 CA 证书的使用。例如，可以使用证书信任列表来建立对一个商业 CA 颁发的证书的信任，并限制这些证书的使用。或者在 Extranet 上使用证书信任列表控制对商业伙伴管理的 CA 颁发的证书的信任。

例如，贵公司可能致力于与另一个公司建立合资企业。该伙伴公司可以为 Web 访问、安全电子邮件和软件签名等等目的颁发自己的证书。而您可能想与该伙伴公司的职员交换安全电子邮件，却又不想为此颁发证书。那么，您可以将该公司的根 CA 添加到企业信任容器中新证书信任列表，指定该伙伴证书将只对电子邮件用途可信任。

配置证书登记和续订

Microsoft 证书服务支持各种登记和续订方法，比如使用证书申请向导的证书申请和使用 Microsoft 证书服务 Web 页的证书申请。但如果您部署了第三方证书服务或自定义证书登记和续订应用程序，就必须执行这些服务和应用程序要求的配置。

开始颁发证书

在要求的证书服务安装和配置好之后，就可以开始为用户、计算机和服务颁发证书了。在开始颁发证书时，请牢记以下方面：

- 证书要颁发给域组策略“ 自动证书申请 ”设置作用域中的计算机。管理员也可以使用证书申请向导和 Microsoft 证书服务 Web 页，为本地计算机手动申请证书。请考虑分阶段安排手动登记，以分散计算机登记的管理工作量。
- 智能卡管理员可以使用 Microsoft 证书服务 Web 页上的“ 智能卡登记站 ”，颁发智能卡证书。考虑分阶段安排智能卡登记，以分散智能卡登记的管理工作量。
- 在使用智能卡前的过渡阶段，通常同时启动智能卡身份验证和 CTRL+ALT+DEL 安全登录顺序两种方式。但由于这会削弱网络的安全性，因此请配置用户帐户策略，以保证一旦智能卡用户培训完毕并可以使用，就必须使用智能卡登录。

在开始颁发证书后，请紧密监视证书服务的性能，以确保 CA 能够处理证书负载。为了纠正过载情况，可以考虑添加更多的颁发 CA，或将证书登记安排到更短的分段。证书续订也能产生过载情况，因此添加更多的 CA 和安排证书登记到更短阶段也能分散高峰续订负载。

公钥基础结构规划任务列表

表 12.4 总结了在规划 PKI 部署时需要执行的任务。

Table 12.4 公钥基础结构规划任务列表

任务	所在章节
明确证书要求	明确您的证书要求
定义颁发证书的程序	定义证书策略和证书颁发机构行为规则
定义 CA 信任层次结构	定义证书颁发机构信任策略
定义对 CA 的安全要求	定义对证书颁发机构的安全要求
定义证书使用周期	定义证书使用周期
定义证书登记和续订程序	定义证书登记和续订程序
定义证书吊销策略	定义证书吊销策略
定义维护策略	定义维护策略
定义灾难恢复策略	制定恢复规划
建立实施计划和日程	部署您的公钥基础结构

第 13 章 - 服务器自动安装与升级

现在，您已经准备好进行 Microsoft® Windows® 2000 Server 及相关应用程序的自动安装了。这是进行任何级别的部署——包括检测、先导测试或生产应用的先决条件。本章介绍了可用的自动安装方法，包括准备要求和示例配置。参与安装过程设计的网络工程师和参与安装 Windows 2000 及相关应用程序的系统管理员都应该熟悉本章内容。

安装 Windows 2000 Server，可以是在尚未安装 Microsoft® Windows® 2000 以前版本操作系统的计算机上进行全新安装，也可以是在当前运行 Microsoft® Windows NT® Server 3.51 或 Microsoft® Windows NT® Server 4.0 的计算机上进行全新安装或升级。本章中的信息将帮助您确定是要进行全新安装还是进行升级。

本章内容

确定进行升级还是全新安装
准备安装
自动安装服务器应用程序
自动安装 Windows 2000 Server
安装配置示例
安装规划任务列表

本章目标

本章将帮助您创建以下规划文档：

- 自动安装规划

资源工具包中的相关信息

- 有关规划的更多信息，请参见本书的“规划概述”。
- 有关管理客户计算机的更多信息，请参见本书中的“定义客户管理与配置标准”。
- 有关客户自动安装的更多信息，请参见本书中的“客户自动安装与升级”。有关本章涉及的无人参与安装参数的更多信息，请参见 Windows 2000 操作系统 CD 中的“Microsoft Windows 2000 Guide to Unattended Setup” (Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，可以使用 Windows “资源管理器”访问该文件。在 Windows 95 及更早版本，或在 MS-DOS 中，可以使用 Extract 命令访问该文件。
- 有关无人参与安装的更多信息，包括示例应答文件，请参见本书附录“无人参与安装的应答文件示例”。

确定进行升级还是全新安装

在企业环境中，在每台计算机上都使用 Windows 2000 的标准交互式安装并不合算。为了大幅降低总拥有成本 (TCO)，您可以在多台计算机上执行 Windows 2000 Server 自动安装。

	关键决定 在进行 Windows 2000 Professional 的自动安装之前，必须确定该安装是从 Windows NT 的升级还是全新安装。

以下两条可以帮助您确定进行升级还是进行全新安装。

- 如果单位已应用了 Windows 操作系统并且对信息技术 (IT) 部门实行集中管理，则可以选择升级。如果您准备创建一个目前还不存在的集中管理环境，则可以选择全新安装，以便在安装时实施标准配置。
- 如果计划使用现有的硬件和软件应用程序，则需要进行升级。相反，如果您计划购买新硬件并安装新的软件应用程序，则需要进行全新安装。

解决关键规划问题

如果计划在尚未安装 Windows 2000 以前版本操作系统的计算机上安装 Windows 2000 Server，显然应该选择全新安装。如果计算机目前正在运行 Windows 95、Windows 98、Windows NT Workstation 3.51 或 Windows NT Workstation 4.0，则需要确定升级现有操作系统和进行全新安装哪个更为合算。

表 13.1 升级或安装之前应解决的规划问题

问题	任务
单位目标	确定公司的主要目标。
区域需求	识别具体的区域需求，并确定商业活动是否会包括国际分支机构或公司。
用户组	分析用户组，包括具体的工作类别和需求、计算机知识及经验、安全性需求、用户位置及其网络连接问题包括链接速度。
应用程序需求	确定哪些产品将预装到所有计算机，哪些公布给特定类型的服务器，而又有哪些分发给特定级别类型的服务器。
硬件	收集现有硬件的清单并预测新硬件需求。 在升级或安装之前设定最低硬件需求。 计划未来的计算机需求。 确定计算机在单位中的使用周期。 确定是否所有计算机都有可引导光盘。
风险和问题范围	明确潜在的风险，包括应用程序和 Windows 2000 不兼容、时间线问题、多个站点、非集中预算或可能面临的合并的影响。
增长预期	确定项目在未来一年、三年和五年的增长预期。同时考虑计划中的合并、新增的站点以及在其它国家的增长计划。
网络问题	确定远程站点是否有应用程序部署服务器。确定中央站点以外的服务器如何升级。
软件管理	确定是否已有软件管理系统，如 Microsoft® Systems Management Server，在其中可以进行部署安排。
连接	确定服务器及其间的连接是否已经建立，可以为公司的所有用户分发大型程序包。

选择安装方法

在解决了规划问题以后，您就可以选择自动安装的方法。表 13.2 列出了自动安装的方法，并显示了它们可用于升级、还是全新安装或者两者都可以。

表 13.2 自动安装方法

方法	Windows 2000 版本	升级	全新安装
Syspart	Server 与 Professional	否	是
Sysprep	Server 与 Professional	否	是
SMS	Server 与 Professional	是	是

可引导 CD	Server 与 Professional	否	是
远程操作系统安装	Professional	否	是

准备安装

准备 Windows 2000 Server 的全新安装，需要做以下工作：

- 创建分发文件夹。
- 了解如何使用应答文件。
- 了解 Windows 2000 安装命令。

备注 本节所述的执行自动安装的原则既适用于全新安装，也适用于升级。最常进行的是全新安装。

图 13.1 是一个显示安装过程的流程图。

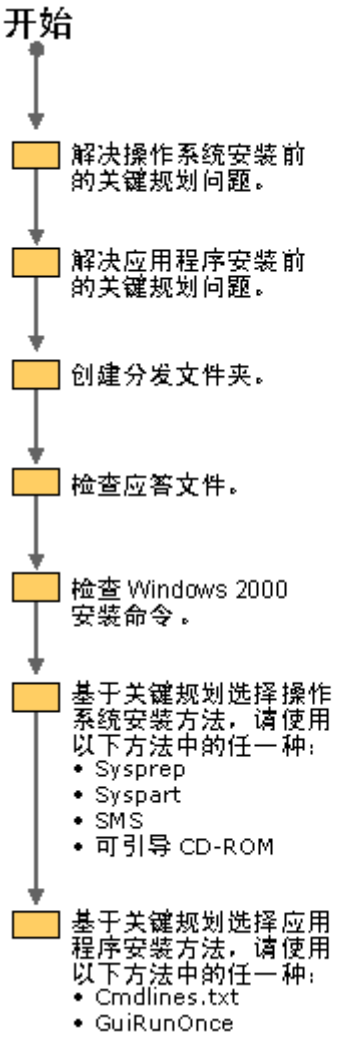


图 13.1 自动安装流程图

创建分发文件夹

为了在网络的多台计算机上安装 Windows 2000 Server，必须创建至少一组分发文件夹。分发文件夹一般位于服务器上，计算机可以连接服务器并通过在目标计算机上运行 Winnt.exe 或 Winnt32.exe 安装 Windows 2000。对不同的系统版本，您可以使用有不同应答文件的同一组分发文件夹。即便使用磁盘映射作为安装方法，以分发文件夹做为起点也可以为不同的系统类型提供一致的执行方法。另外，您还可以通过修改分发文件夹中的文件，或修改应答文件产生新的映射、更新映像，而无需再从头开始。

为了帮助服务器负载平衡及让 Microsoft® Windows® 95、Windows 98、Windows NT、或 Windows 2000 计算机上的 Windows 2000 安装的文件复制过程更快，您可以在多台服务器上创建分发文件夹。然后就可以运行带有多至八个源文件位置的 Winnt32.exe 命令。有关安装命令的更多信息，请参见本章后面的“检查 Windows 2000 安装命令”。

备注 本章中，Windows NT 一词既指 Microsoft® Windows NT® 3.51 也指 Microsoft® Windows NT® 4.0。

分发文件夹包含了 Windows 2000 Server 或 Microsoft® Windows® 2000 Advanced Server 安装文件，以及设备驱动程序和其它安装所需的文件。

Setup Manager 是 Windows 2000 Server CD 上提供的工具，可以帮助您使创建分发文件夹的的过程自动化。有关 Setup Manager 的更多信息，请参见本章后面的“检查应答文件”。

备注 本章中，“Windows 2000 安装程序”也称做“安装程序”。

要创建分发文件夹，请

1. 连接到要在上面创建分发文件夹的网络服务器。
2. 在网络服务器的分发共享点创建 \i386 文件夹。

   为了帮助区分不同版本 Windows 2000 （ Microsoft® Windows® 2000 Professional、Microsoft® Windows® 2000 Server 和 Microsoft® Windows® 2000 Advanced Server ） 的多个分发共享点，可以给文件夹选择其它名称。如果想在单位的各国际分支机构使用本地语言版本的 Windows 2000，可以为每个本地版本分别创建分发共享点。
3. 将 \i386 文件夹的内容从 Windows 2000 Server CD 复制到已创建的文件夹。
4. 在已创建的文件夹中，创建名为 \OEM 的子文件夹。

   安装过程中，\OEM 子文件夹会为要复制到目标计算机上的附件文件提供必要的文件夹结构。这些文件包括驱动程序、工具、应用程序和任何其它单位部署 Windows 2000 Server 时需要的文件。

构建分发文件夹

图 13.2 显示了一个分发文件夹结构的示例。

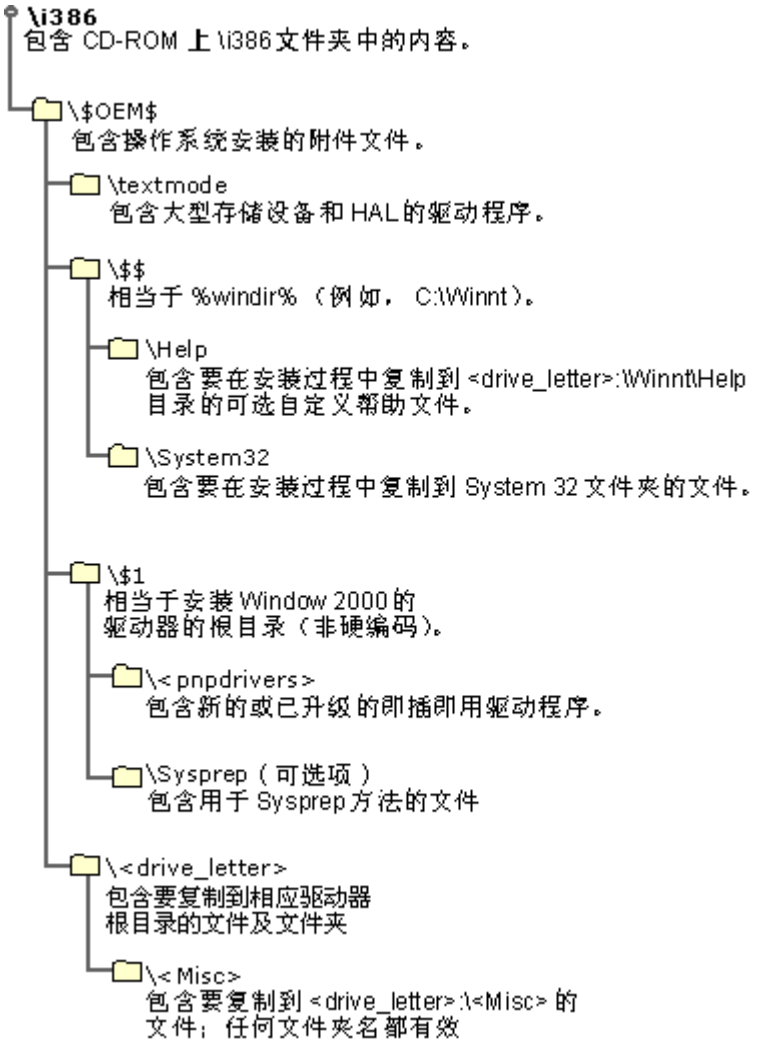


图 13.2 分发文件夹结构示例

\I386

这是分发文件夹，包含了安装 Windows 2000 需要的所有文件。请把 Windows 2000 Server CD 上 \i386 文件夹中的内容复制到该目录，完成分发共享点根目录下分发文件夹的创建。

\OEM

请直接在 \I386 文件夹下创建 \$OEM$ 子文件夹。在安装过程中，自动安装过程需要的目录、标准 8.3 格式文件以及工具可以自动复制到 \$OEM$ 子文件夹。

注意，如果在应答文件中使用 OEMFILESPATH 关键字，可以在分发文件夹以外创建 \OEM 子文件夹。在本章后面的“检查应答文件”中，有应答文件的定义。有关应答文件参数和语法的更多信息，请参见 Microsoft Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。 在 Windows 98 或 Windows 2000 中，请使用 Windows “资源管理器”访问该文件。在 Windows 95 及更早版本中，及在 MS-DOS 中，请使用 Extract 命令访问该文件。

\OEM 可以包含可选文件 Cmdlines.txt，该文件包含了可以在安装的图形用户界面 (GUI) 部分运行的命令列表。这些命令可以用来安装附加工具。有关 Cmdlines.txt 文件的更多信息，请参见本章后面的“使用 Cmdlines.txt ”。

安装程序一旦发现分发点根目录下的 \OEM 子文件夹，就会把该目录下的所有文件复制到安装过程文本部分创建的一个临时目录中。

备注 本章中，安装的 GUI 部分称做 “ GUI 模式 ”，安装的文本部分称做 “ 文本模式 ”。

\OEM\Textmode

\OEM\Textmode 子文件夹包含了安装大型存储设备驱动程序和硬件抽象层 (HAL) 需要使用的新文件的或已更新的文件。这些文件可以包括 OEM HAL、小型计算机系统接口 (SCSI) 设备驱动程序，及引导这些组件加载和安装的 Txtsetup.oem 文件。

请确认其中已包括了 Txtsetup.oem 文件。\OEM\Textmode 子文件夹中的所有文件 (HAL、驱动程序和 Txtsetup.oem) 必须在应答文件的 [OEMBootFiles] 段列出。

\$OEM$\$$

\$OEM$\$$ 子文件夹与 %systemroot% 或 %windir% 环境变量对应。该子文件夹包含了要复制到 Windows 2000 安装目录不同子文件夹中的附加文件。它的结构必须符合标准的 Windows 2000 安装，\$OEM$\$$ 对应 %systemroot% 或 %windir% (例如 C:\Winnt) ，\$OEM$\$$\System32 对应 %windir%\System32，依次类推。每个子文件夹都要包含要复制到目标计算机相应系统文件夹中的文件。

\$OEM$\$1

\$OEM$\$1 对 Windows 2000 而言是一个新的子文件夹，它指向安装 Windows 2000 的驱动器。$1 一词和 %systemdrive% 环境变量对应。例如，如果正在 D 驱动器上安装 Windows 2000，\$OEM$\$1 指向 D。

\$OEM$\$1*Pnpdrvrs*

\$OEM$\$1\Pnpdrvrs 子文件夹对 Windows 2000 而言也是新的，可以在其中放置新的或经过更新的即插即用设备驱动程序。这些文件夹将复制到目标计算机上的 %systemdrive%\Pnpdrvrs。通过把 OemPnPDriversPath 参数添加到应答文件，可以让 Windows 2000 在所创建的文件夹中寻找（在安装过程中或安装之后）新的或是经过更新的即插即用驱动程序以及系统本来就有的驱动程序。注意，您可以用少于八个字符的名称替代 Pnpdrvrs。

\$OEM$\$1\Sysprep

\$OEM$\$1\Sysprep 子文件夹是可选项。该子文件夹包含了运行 Sysprep 工具用到的文件。这些文件将在本章后面 “ 使用 Sysprep 复制磁盘 ” 中描述。

\OEM*Drive_letter*

在文本模式下， \$OEM$\Drive_letter 子文件夹结构都复制到目标计算机相应驱动器的根目录下。例如，\$OEM$\D 子文件夹中的文件将被复制到 D 驱动器根目录下。您也可以在这些子文件夹中再创建子文件夹。例如，\$OEM$\E\Misc 将使安装程序在 E 驱动器上创建一个 \Misc 子文件夹。

需要重命名的文件必须在 $$Rename.txt 中列出。有关文件重命名的更多信息，请参见本章后面的 “ 使用 $$Rename.txt 转换文件名大小 ”。注意，分发文件夹中，文件必须使用短文件名 (8.3 格式）。

安装大型存储设备

在 Windows 2000 中，即插即用功能会检测并安装大部分硬件设备，并在安装的以后阶段将其装载。但对于大型存储设备如硬盘，必须正确安装才能在 GUI 模式阶段得到完全的即插即用支持。

备注 如 Windows 2000 已经支持某种设备，则不需要再另外指定。

为了在文本模式阶段安装 SCSI 设备——即，在得到完全即插即用支持之前——必须提供一个 Txtsetup.oem 文件，来说明安装程序安装特定 SCSI 设备的方式。

重要提示 在使用升级驱动程序之前，请先确认它们已经经过注册。如未注册，安装将会失败。可以分别检测“设备管理器”中每个驱动程序的注册情况，也可以运行 Sigverif.exe，它将在 %windir% 子文件夹中生成一个 Sigverif.txt 文件。Sigverif.txt 会列出系统中所有驱动程序的注册状态。

要安装大型存储设备，请

1. 在分发文件夹 \OEM 子文件夹中，创建 \Textmode 子文件夹。

   将以下文件（可以从设备供应商那里获得）复制到 \Textmode 子文件夹（用适当的驱动程序名代替 *Driver*）：

   - Driver.sys
   - Driver.dll
   - Driver.inf
   - Txtsetup.oem

   备注 某些驱动程序，如 SCSI 小型端口驱动程序，可能不包括 .dll 文件。

2. 在应答文件中，创建 [MassStorageDrivers] 段，并在其中加入需要包括的驱动程序项。例如，[MassStorageDrivers] 段中的项可能是 ：

   ```
   "Adaptec 2940U" = "OEM"
   ```

   该段信息可从 Txtsetup.oem 文件获得，该文件是硬件制造商提供的。

   有关应答文件参数和语法的更多信息，请参见 Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，请使用 Windows “资源管理器”访问该文件。在 Windows 95 和更早版本中，及在 MS-DOS 中，请使用 Extract 命令访问该文件。

3. 在应答文件中，创建 [OEMBootFiles] 段，并在其中键入 OEM\Textmode 文件夹中的文件列表。例如：

   ```
   [OEMBootFiles]<Driver>.sys<Driver>.dll<Driver>.infTxtsetup.oem
   ```

   这里，<Driver> 为驱动程序名。

4. 如果大型存储设备是即插即用设备，它会在 Txtsetup.oem 文件中加入 [HardwareIds.Scsi.yyyyy] 段。如果您的大型存储设备没有这样一段，就需要创建并在其中键入以下项：

   ```
   id = "xxxxx", "yyyyy"
   ```

   在这里，xxxxx 代表设备 ID，而 yyyyy 代表与该设备相关的服务。

   例如，为了安装设备标识符 (ID) 为 PCI\VEN_1000&DEV_0001 的 Symc810 驱动程序，首先要验证 Txtsetup.oem 文件包含以下附加段：

   ```
   [HardwareIds.scsi.symc810]
   id = "PCI\VEN_1000&DEV_0001", "symc810"
   ```

安装硬件抽象层

为了安装指定硬件抽象层 (HAL),需要供应商提供一个 Txtsetup.oem 文件和 HAL 文件。安装大型存储设备驱动程序时，必须使用同一 Txtsetup.oem 文件。由于只能使用一个 Txtsetup.oem 文件，因此如果要同时安装 HAL 和大型存储设备，需要将这些项并入一个文件。

为了使用第三方驱动程序，也必须对应答文件进行适当的修改。有关应答文件参数和语法的更多信息，请参见 Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，可以使用 Windows “资源管理器”访问该文件。在 Windows 95 及更早版本中，或是从 MS-DOS 中，可以使用 Extract 命令访问该文件。

要安装 HAL，请

1. 如果还没有在 \OEM 文件夹中创建 \Textmode 子文件夹，现在创建该文件夹。
2. 把从设备供应商处收到的文件复制到 \Textmode 子文件夹。
3. 在应答文件中，为 HAL 编辑 [Unattend] 段，并加入要安装的驱动程序。例如：

   ```
   [Unattend]Computertype = "<HALDescription >", OEM
   ```

   <HALDescription> 信息可以从驱动程序供应商提供的 Txtsetup.oem 文件 [Computer] 段得到。
4. 在应答文件中，创建 [OEMBootFiles] 段，然后输入 OEM\Textmode 文件夹中的文件名。

安装即插即用设备

以下过程显示了如何安装不是大型存储设备，也不是 HAL，也没有包括在 Windows 2000 操作系统 CD 上的即插即用设备。

要安装即插即用设备，请

1. 在分发文件夹中，为特殊即插即用驱动程序及其 .inf 文件创建子文件夹。例如，可以创建一个名为 PnPDrvs 的文件夹：

   ```
   $OEM$\$1\PnPDrvs
   ```
2. 通过在应答文件中添加下行内容，增加即插即用驱动程序列表的搜索路径。

   ```
   OEMPnPDriversPath = "PnPDrvs"
   ```

   如果 PnPDrvs 文件夹包含子文件夹，必须为每个子文件夹指定路径。路径必须以分号隔开。

   为了方便维护文件夹，使它们适应以后的设备驱动程序，一定要为潜在的设备驱动程序创建子文件夹。通过把文件夹分成子文件夹，可以按设备类型来存储设备驱动程序文件，而不用把所有的设备驱动程序文件放在一个文件夹中。建议这些子文件夹包括 Audio、Modem、 Net、 Print、 Video 等。 而另一个子文件夹可以存储目前尚未知道的新硬件设备。

   例如，如果 PnpDrvs 文件夹包含子文件夹 Audio、Modem 和 Net,应答文件必须包含下行内容：

```
OEMPnPDriversPath = "PnPDrvs\Audio;PnPDrvs\Modem;PnpDrvs\Net"
```

使用 $$Rename.txt 转换文件名大小

在安装过程中，$$Rename.txt 文件会把短文件名改为长文件名。$$Rename.txt 列出了特定文件夹中所有需要重命名的文件。包含短文件名并需要转换的文件夹都必须包含自己的 $$Rename.txt 版本。

为了使用 $$Rename.txt，请把该文件放入需要转换文件名的文件夹中。$$Rename.txt 的语法如下：

```
[section_name_1]
short_name_1 = "long_name_1"
short_name_2 = "long_name_2"

short_name_x = "long_name_x"

[section_name_2]
short_name_1 = "long_name_1"
short_name_2 = "long_name_2"

short_name_x = "long_name_x"
```

参数定义如下：

- section_name_x——包含这些文件的子文件夹的路径。段可以不需要命名，或者可以用反斜线 （\） 作为名称，表示该段包含驱动器根目录下的文件名或子文件夹名称。
- short_name_x——子文件夹中需要重命名的文件或子文件夹名称。该名称不能加引号。
- long_name_x——文件或子文件夹的新名称。该名称如果包含空格或逗号，则必须加引号。

提示 如果使用 MS-DOS 启动安装，而 MS-DOS 工具无法复制路径名称多于 64 个字符的文件夹，则可以使用短文件名，然后用 $$Rename.txt 重新命名。

检查应答文件

应答文件是一个自定义脚本，负责应答安装程序提出的问题，而无需用户输入。Windows 2000 Server CD 包含一个示例应答文件，您可以编辑和使用它。应答文件通常以 Unattend.txt 命名,您也可以为它重新命名。（例如，只要在 setup 命令中正确指定，Comp1.txt、Install.txt 和 Setup.txt 都是应答文件的有效名称）。这让您在需要为单位的不同部分维护不同脚本的安装时，可以建立并使用多个应答文件。注意，应答文件也可以被其它程序使用，如 Sysprep 会使用可选的 Sysprep.inf 文件 。

应答文件会告诉安装程序如何与分发文件夹及已创建的文件进行互动。例如，在应答文件的 [Unattend] 段有一个 OEMPreinstall 项，它会让安装程序把 OEM 子文件夹从分发文件夹复制到目标计算机上。

应答文件包含多个可选段，您可以对它们作出修改，提供满足您的安装要求的信息。应答文件会在一个 Windows 2000 标准互动式安装过程中，为安装程序提供所有问题的答案。在 Unattend.doc 文件中，包括了有关应答文件关键字及其值的详细信息。有关应答文件段及其相关参数的更多信息，请参见 Windows 2000 操作系统 CD 上的“ Microsoft Windows 2000 Guide to Unattended Setup” (Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，请使用 Windows “ 资

源管理器”访问该文件。在 Windows 95 及更早版本中，或是从 MS-DOS 中，请使用 Extract 命令访问该文件。

为了进行 Windows 2000 Server 无人参与安装，必须创建一个应答文件，并在安装过程通过可引导 CD 的方法，或通过运行 Winnt.exe 或 Winnt32.exe 指定该文件。以下是使用 Winnt.exe 的 setup 命令的示例。

```
Winnt /S:Z:\I386 /U:Z:\unattend.txt
```

注意 /U 的使用：它是一个命令行开关，与 **Winnt** 命令一起使用时表明要进行无人参与安装（ **/unattend** 是与 **Winnt32** 命令一起使用的参数，它告诉安装程序以无人参与模式运行）。有关 Winnt.exe 和 Winnt32.exe 的更多信息，请参见本章后面的“检查 Windows 2000 安装命令”。

创建应答文件

应答文件是一个自定义脚本，可以用它来运行 Windows 2000 Server 的无人参与安装。创建应答文件有两种方式：一种是使用 Setup Manager，另一种为手动创建。

使用 Setup Manager 创建应答文件

为了帮助您创建或修改应答文件，Microsoft® Windows® 2000 Server Resource Kit 伙伴 CD 上提供了一个 Setup Manager 应用程序（\Support\Tools 文件夹中的 Deploy.cab 文件中）。使用 Setup Manager，可以增加创建或更新应答文件过程的一致性。

Setup Manager 可以用来完成以下任务，其结果将成为应答文件参数。

- 指定应答文件的平台（ Microsoft® Windows® 2000 Professional、Windows 2000 Server、远程操作系统安装或 Sysprep ）。
- 指定无人参与安装模式的自动级别。（这些级别包括“提供默认值”、“完全自动”、“隐藏页面”、“只读” 和“ GUI 模式安装”。”
- 指定默认用户信息。
- 定义计算机名选项，包括 /UDF 以访问包含有效计算机名的文件。
- 配置网络设置。
- 创建分发文件夹。
- 添加自定义徽标和背景文件。
- 把文件添加到分发文件夹。
- 把命令添加到 [GuiRunOnce] 段。
- 创建 Cmdlines.txt 文件。
- 指定代码页。
- 指定区域选项。
- 指定时区。
- 指定 TAPI 信息。

Setup Manager 不能实现以下功能：

- 指定系统组件，如 Internet 信息服务 (IIS)。
- 创建 Txtsetup.oem 文件。
- 在分发文件夹中创建子文件夹。

表 13.3 描述了由 Setup Manager 创建的最常用的应答文件格式。

表 13.3 Setup Manager 创建的应答文件格式

参数	目的
安装路径	在要安装 Windows 2000 Server 的目标计算机上指定想要的路径。
升级选项	指定从 Windows 95、Windows 98、Windows NT 还是从 Windows 2000 升级。
目标计算机名	指定用于目标计算机的用户名、单位名和计算机名。
产品 ID	指定从产品文档中得到的产品标识号。
工作组或域	指定计算机所属的工作组或域的名称。
时区	为计算机指定时区。
网络配置信息	指定网络适配器类型和包括网络协议的配置。

备注 安装 Windows 2000 Server 时，不要求先创建域控制器。您可以先创建成员服务器，并在以后用 Active Directory 安装向导 (dcpromo.exe) 将其提升为域控制器。

手动创建应答文件

要手动创建应答文件，可以使用“ 记事本 ”之类的文本编辑器。一般来说，应答文件包括段标题、参数和这些参数的值。尽管大多段标题都是事先定义的，但您也可以定义其它的段标题。注意，如果安装不要求的话，就不必在应答文件中指定所有可能的参数。

无效的参数值在安装程序完成以后会产生错误或导致不正确行为。

应答文件格式如下：

```
[section1]
;
; Section contains keys and the corresponding
; values for those keys/parameters.
; Keys and values are separated by ' = ' signs.
; Values that have spaces in them usually require double quotes
; "" around them.
;
key = value
.
.
[section2]
key = value
.
.
```

使用应答文件设置密码

在安装中使用应答文件，可以为以下密码命令设置参数：

- AdminPassword
- UserPassword
- DefaultPassword

- DomainAdminPassword
- AdminstratorPassword
- Password

有关这些命令的定义，请参见 Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，请使用 Windows “资源管理器”访问该文件。在 Windows 95 或更早版本中，或是从 MS-DOS 中，请使用 **Extract** 命令访问该文件。另外，在附件“无人参与安装的应答文件示例”中，可以找到使用某些参数的应答文件示例。

备注 密码只限于 127 个字符。如果指定了多于 127 个字符的密码，则将造成密码无效，并无法登录系统。

在安装完成之后，包含计算机所有配置设置的应答文件留在计算机上；但所有的密码信息将从应答文件的本地副本中删除，从而不会造成安全泄密。

警告 在安装过程中，应答文件可以从硬盘上得到。如果您对安全有所顾虑，就不要把密码信息加到无人参与安装的应答文件中。

通过运行一些包含原应答文件参数的命令，本地应答文件让您可以自动设置可选组件。这些组件可以包括：把服务器配置成域控制器、群集服务器，或者启用消息队列。

扩展硬盘分区

在安装开始阶段，您可以选择一个小的分区（大约较大磁盘上的 1 GB），然后在 Windows 2000 安装过程中使用应答文件中的 ExtendOEMPartition 参数扩展这一分区。ExtendOEMPartition 参数只对 NTFS 分区可用。它既能用于常规应答文件中，也能用于基于 Sysprep 安装的应答文件。

有关 Sysprep 和 Sysprep.inf 文件的更多信息，请参见本章后面的“使用 Sysprep 复制磁盘”。

备注 ExtendOEMPartition 只在活动系统分区上起作用。在同一硬盘的其它分区上，或是计算机的不同硬盘上，它不起作用。另外，当使用 ExtendOemPartition=1 时，它会将分区扩展到硬盘上所有剩余空间，并将最后一个磁道留为空白。这是有意设计的，目的是让您可以启用动态卷。

如果是在文件分配表 (FAT) 分区上进行无人参与安装的过程中使用 ExtendOEMPartition，则在应答文件的 [Unattended] 段中需要指定 File System=ConvertNTFS，以便首先把分区转换成 NTFS。如果是在基于 Sysprep 的安装中使用 ExtendOEMPartition，请参见本章后面的“使用 Sysprep 复制磁盘”。

有关使用 ExtendOemPartition 的更多信息，请参见 Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，请使用 Windows “资源管理器”访问该文件。在 Windows 95 及早期版本中，或是从 MS-DOS 中，请使用 **Extract** 命令访问该文件。

将应答文件用于 Active Directory 安装向导

安装 Windows 2000 Server 以后，可以使用 Active Directory 安装向导，自动化创建域控制器的过程。要做到这一点有两种方法：

- 从 Unattend.txt 应答文件的 [GuiRunOnce] 段运行以下命令：

```
dcpromo.exe
```

- 使用附件“无人参与安装的应答文件示例”[DCInstall]段中定义的命令，创建一个特殊应答文件，然后运行以下命令：

  ```
  dcpromo.exe /answer:answer_file_name
  ```

有关 Active Directory 安装向导的更多信息，请参见本书中的“确定域迁移策略”。

检查 Windows 2000 安装命令

为了安装 Windows 2000，必须运行合适的 Windows 2000 Setup 程序，Winnt.exe 或者 Winnt32.exe。在本章中，Winnt.exe 和 Winnt32.exe 都称作“安装程序”。需要运行的安装程序类型可以如下确定：

- 对于从 MS-DOS 或 Microsoft® Windows® 3.*x* 计算机上进行的全新安装，请从 MS-DOS 命令行运行 Winnt.exe。
- 对于从 Windows NT、Windows 95 或 Windows 98 进行的全新安装或升级，请运行 Winnt32.exe。

注意，您可以直接从启动软盘开始一个标准交互式安装，该启动软盘是与 Windows 2000 Server CD 一起交付的。

警告 如果在升级到 Windows 2000 之前，进行应用程序的升级，请务必在运行安装程序之前重新启动计算机。

有关安装方法的更多信息，请参见本章后面的“Windows 2000 Server 自动安装”。

Winnt.exe

Winnt.exe 命令以及用于自动安装的参数，如下所示：**winnt** [**/S**[:*sourcepath*]][**/T**[:*tempdrive*]]**/U**[:*answer_file*]][**/R**[*x*]:*folder*][**/E:***command*]

有关参数定义和命令语法，请参见本书附录“安装命令”。

对于有多个分区的硬盘驱动器，如果分区有足够空间的话，安装程序 Winnt.exe 会把 Windows 2000 安装在活动分区上。否则，安装程序会搜寻其它包含足够空间的分区，并提示您选择想要的分区。对自动安装，可以运行带 **/T** 参数的安装程序绕过提示，自动指向需要的分区。例如：

```
winnt [/unattend] [:<path>\answer.txt] [/T[:d]]
```

Winnt32.exe

Winnt32.exe 命令以及用于自动安装的参数，如下所示：

```
winnt32 [/s:sourcepath] [/tempdrive:drive_letter]
[/unattend[num][:answer_file]] [/copydir:folder_name]
[/copysource:folder_name] [/cmd:command_line]
[/debug[level][:filename]]
[/udf:id[,UDB_file]] [/syspart:drive_letter] [/noreboot]
[/makelocalsource] [/checkupgradeonly] [/m:folder_name]
```

有关参数定义和命令语法，请参见本书附录 B“安装命令”。

对于有多个分区的硬盘驱动器，如果分区包含足够空间的话，安装程序 Winnt32.exe 会把 Windows 2000 安装在活动分区。否则，安装程序会搜寻其它包含足够空间的分区，并提示选择

想要的分区。对自动安装，您可以运行有 **/tempdrive** 参数的安装程序绕过提示，自动指向想要的分区。例如：

```
winnt32 [/unattend] [:<path>\answer.txt] [/tempdrive:d]
```

Windows 2000 可以使用多达八个 /S 开关，以指向其它分发服务器，作为目标计算机安装的源位置。这种功能有助于加快目标计算机安装的文件复制，同时为运行安装程序的分发服务器提供了额外的负载平衡能力。例如：

```
<path to distribution folder 1>\winnt32 [/unattend]
[:<path>\answer.txt] [/s:<path to distribution folder 2>] [/s:<path
to distribution folder 3>] [/s:<path to distribution folder 4]
```

表 13.4 显示了安装命令以及如何用于 Windows 2000。

表 13.4 使用安装命令

安装命令	Windows 2000 版本	升级	全新安装
Winnt.exe	Server 和 Professional	否	是
Winnt32.exe	Server 和 Professional	是	是

服务器应用程序自动安装

在解决了关键的规划问题后，您就可以决定如何进行服务器应用程序的自动安装了。大多情况下，我们都愿意使用应用程序的无人参与安装功能完成安装。

可以选择以下方法：

- Cmdlines.txt
- 从应答文件的 [GuiRunOnce] 段运行应用程序安装程序或者批处理文件。

使用 Cmdlines.txt

Cmdlines.txt 文件包含了一些命令，GUI 模式在安装可选组件（比如安装 Windows 2000 Server 之后必须立即安装的应用程序）时会执行这些命令。如果计划使用 Cmdlines.txt，需要将其放入分发文件夹的 \$OEM$ 子文件夹中。如果使用 Sysprep，请把 Cmdlines.txt 放入 \$OEM$\$1\Sysprep 子文件夹中。

当以下条件满足时，请使用 Cmdlines.txt：

- 从分发文件夹中的 \OEM 子文件夹进行安装。
- 安装的应用程序具有以下属性：

  它不能配置为多用户模式——例如， Microsoft® Office 95。

  – 或 –

  它已设计成由一个用户安装，并复制用户特定信息。

Cmdlines.txt 的语法如下所示：

```
[Commands]
"command_1"
"command_2"
.
```

.
"*command_x*"

参数定义如下：

- "*command_1*"、"*command_2*"... "*command_x*" 指 GUI 模式调用 Cmdlines.txt 时，希望运行的命令（及运行的顺序）。注意，所有的命令必须在引号内。

使用 Cmdlines.txt 时，要注意以下情况：

- 在 Cmdlines.txt 中的命令在安装阶段执行时，不会有用户登录，并不能保证网络连接。因此，用户特定信息将写入默认用户注册表，以后创建的用户也会收到该信息。
- Cmdlines.txt 要求将应用程序或工具运行所需的文件放在安装过程可以访问的目录中，即这些文件必须在硬盘上。

使用应答文件的 [GuiRunOnce] 段

应答文件的 [GuiRunOnce] 段包含了安装程序运行后，用户第一次登录到计算机上时要运行的命令列表。例如，可以在 [GuiRunOnce] 段中输入下行内容，以启动应用程序自动安装程序：

```
[GuiRunOnce]
"%systemdrive%\ <appfolder>\<appinstall> -quiet"
```

如计划使用 [GuiRunOnce] 启动安装过程，还需要考虑其它一些因素：

如应用程序强制重新启动，请确定是否有禁止重新启动的方法。这很重要，因为系统每次重新启动，[GuiRunOnce] 段中以前的所有项目都将丢失。如果在 [GuiRunOnce] 以前列出的项尚未完成，系统重新启动后，剩余的项将不再运行。如果应用程序内部无法禁止重新启动，可以尝试把应用程序重新打包成“ Windows 安装服务 ”程序包。一些第三方产品也提供了这一功能。

Windows 2000 同时还附带了 WinINSTALL LE （限制版本），这是一个“ Windows 安装服务 ”的重新打包工具。WinINSTALL LE 让您可以把 Windows 以前的安装服务应用程序有效地重新打包成可以用“ Windows 安装服务 ”分发的程序包。有关 WinINSTALL LE 的更多信息，请参见 Windows 2000 Server CD 上的 \Valueadd\3rdparty\Mgmt\Winstle 文件夹。

有关 Windows 安装服务打包的更多信息，请参见本书中的“ 客户自动安装与升级 ”。

重要提示 如果把应用程序安装到多个 Windows 2000 本地化语言版本，建议您在本地化版本上测试重新打包的应用程序，以确保应用程序把文件复制到了正确的位置并正确写入注册表项目。

如果应用程序要求安装 Windows “ 资源管理器 ” 外壳，[GuiRunOnce] 段不再有效，因为在执行 Run 和 RunOnce 命令时还没有载入外壳。请与应用程序供应商核实是否有适合在这种情况下应用程序安装的升级版本，或补丁程序。如果没有，可以将应用程序重新打包成“ Windows 安装服务 ”程序包，或使用其它的分发方法。

使用同类安装机制的应用程序，如果不使用 /wait 命令也可能不能正常运行。应用程序安装正在运行，而又启动了另一进程的情况下，可能发生这种情况。安装程序例程还在运行时，初始化其它的进程或关闭当前的活动进程，都可能导致 RunOnce 段注册表项中列出的下一个例程启动。由于有一个以上的安装机制实例同时运行，第二个应用程序通常会失败。有关如何使用批处理文件控制这一问题的示例，请参见本章后面的“ 使用批处理文件控制多个应用程序的安装 ”。

使用应用程序安装程序

预装应用程序的首选方法，是使用与应用程序一起提供的安装程序例程。如果预装的应用程序可以在安静模式（无用户干预）下使用 **/q** 或 **/s** 命令行开关，就可以这样做。请参见应用程序帮助文件或文档，了解安装机制支持的命令行参数列表。以下是一个命令行示例，您可以将其放进 [GuiRunOnce] 段，以让应用程序安装程序本身启动无人参与安装。

```
<path to setup>|Setup.exe /q
```

安装程序参数会因应用程序的不同而不同。例如，一些应用程序中的 **/l** 参数会在创建日志文件监视安装时有用。一些应用程序会拥有防止自动重启的命令。这可以有助于用最少的重新启动控制应用程序的安装，。

在预装任何应用程序以前，请务必与应用程序供应商核实相关信息、说明、工具以及最佳做法。

重要提示 对任何应用程序，不论如何安装，都必须满足其许可证要求。

使用批处理文件控制多个应用程序的安装

要控制多个应用程序的安装，可以创建一个包含很多独立安装命令的批处理文件，并使用 **Start** 命令和 **/wait** 命令行开关。这种方法可以保证应用程序按既定顺序安装，每个应用程序在下一应用程序开始安装之前已经安装完毕。批处理文件会从 [GuiRunOnce] 段开始运行。

以下程序说明了如何创建批处理文件、如何安装应用程序、以及如何在应用程序安装完成后删除批处理文件的所有索引。

要使用批处理文件安装应用程序，请

1. 创建包含类似以下各行内容的批处理文件：

   ```
   Start /wait <path to 1st application>\<Setup> <command line
   parameters>
   Start /wait <path to 2nd application>\<Setup> <command line
   parameters>
   Exit
   ```

   这里：

   - <path> 是启动安装程序的可执行文件的路径。该路径在安装过程中必须可用。
   - <Setup> 是启动安装程序的可执行文件的名称。
   - <command line parameters> 是适合应用程序的安静模式参数。

2. 把批处理文件复制到分发文件夹或其它安装过程可以访问的位置。

3. 以 <filename>.bat 作为批处理文件名，在应答文件 [GuiRunOnce] 段中加入一项以运行批处理文件，见下例。该示例假设批处理文件已经复制到本地硬盘的 Sysprep 文件夹，当然它可以放在安装程序可以访问的任何其它位置。

   ```
   [GuiRunOnce]
   "%systemdrive%\sysprep\<filename>.bat"
   "<path-1>\<Command-1>.exe"
   "<path-n>\<Command-n>.exe"
   "%systemdrive%\sysprep\sysprep.exe –quiet"
   ```

   这里：

- o <path-1>\<Command-1.exe> 和 <path-1>\<Command-n.exe> 是附加应用程序及工具的安装或配置工具的完全路径。也可以是其它批处理文件的路径。这些路径在安装过程必须可用。

Windows 2000 Server 自动安装

在企业环境中，在每台计算机上都进行 Windows 2000 的标准交互式安装并不合算。为了大幅度降低总拥有成本 (TCO)，可以在多台计算机上执行 Windows 2000 Server 自动安装。

您可以进行以下类型的自动安装：

- Windows 2000 Server 的核心操作系统。
- 任何不作为服务运行的应用程序。
- 不同语言包安装过程中的 Windows 2000 Server 附加语言支持。
- Windows 2000 Server 服务包。

Windows 2000 Server 自动安装需要使用应答文件运行安装程序。安装程序能以无人参与方式运行。无人参与安装程序包含以下步骤：

- 创建应答文件。
- 确定并进行配置计算机特定信息的过程。
- 确定并进行使选择的分发方法（比如使用网络分发点或硬盘复制）自动化的过程，。

自动安装的新选项

Windows 2000 自动安装中有几个新的选项，在应答文件中可用这些选项来控制运行的程序及运行的方式。有关应答文件参数和语法的更多信息，请参见 Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，请使用 Windows “资源管理器”访问该文件。在 Windows 95 及早期版本，或是从 MS-DOS 中，请使用 **Extract** 命令访问该文件。

柔性网络 Windows 2000 中，有几个柔性网络配置，包括对协议、服务和客户的附加支持。有了这种柔性网络配置，就可以设置绑定顺序，容易地设置默认信息并在系统中安装多个网卡。另外，为使安装和配置更容易，Windows 2000 可以自动安装并配置网络设备驱动程序。默认情况下，Windows 2000 会为系统中每个网卡安装默认组件，除非在应答文件中另外指定。默认网络组件包括 Microsoft Networks 客户、TCP/IP、Microsoft 网络文件和打印共享，以及启用动态主机配置协议 (DHCP)。

自动登录能力 您可以自定义应答文件，让计算机在安装完成首次启动 Windows 2000 时，或是在之后的特定次数，可以管理员方式自动登录。如果需要 Windows 2000 可以在特定次数自动登录，以完成 RunOnce 项中进行的任务，则需要在应答文件中提供一个非空的管理员密码 (AdminPassword)。 然后用 AutoAdminLogonCount 指定需要系统自动登录的次数。如使用了空密码，而在以后重新启动时不用其它方法提供凭信，则安装程序只能自动登录到系统一次。这样做是为了降低安全风险。注意，如果在文本文件中提供了管理员帐户凭信，而用户可以访问该文件，则会产生安全风险。

自动命令执行 应答文件的 [GuiRunOnce] 段包含了要在 GUI 模式完成后作为安装程序的一部分继续执行的命令列表。使用 [GuiRunOnce]，可以指定要安装的应用程序、配置系统的工具、或首次登录安装好的计算机时要运行的工具列表。

简化的时区规范　在应答文件中，您可以更容易地指定计算机时区，与 Windows NT 相比，只需更少的调试。通过列举可能的时区，出错的机会更少了，因为您不再需要输入完整的时区字符串。

增强的区域和语言设置 在应答文件中，您可以指定系统和用户位置、键盘和输入方法以及要安装的语言支持。Setup Manager 让您可以在向导的 GUI 界面上选择希望安装在系统上的设置，从而简化了这一过程。

简化的设备预装 由于引入了即插即用功能、OemPnPDriversPath 关键字、新的分发共享点结构，预装设备变得更为简单，只需要把新驱动程序添加到分发共享点的一个文件夹并指定 OemPnPDriversPath 关键字。

自动安装方法

可以用不同的方法运行 Windows 2000 Server 自动安装。正如本章前面所述，方法的选择取决于关键规划的结果。

在服务器上执行自动安装的方法包括：

- 在硬件配置不同的计算机上使用 Syspart。
- 使用 Sysprep 复制磁盘。
- 使用 Systems Management Server。
- 使用可引导 CD。

表 13.5 说明了何时使用这些自动安装方法。

表 13.5 何时使用自动安装方法

方法	用途
Syspart	Syspart 用于硬件配置不同计算机的全新安装。
Sysprep	主控计算机和目标计算机有相同硬件（包括 HAL 和大型存储设备控制器）时，使用 Sysprep。
Systems Management Server	Systems Management Server 用于实现 Windows 2000 Server 对多个系统的升级管理，尤其是在这些系统地点分散时。
可引导 CD	在基本输入/输出系统 (BIOS) 允许从 CD 启动的计算机上，可以使用可引导 CD 的方法。

在硬件配置不同的计算机上使用 Syspart

Syspart 通过 Winnt32.exe 的一个可选参数运行。如果主控计算机和要安装 Windows 2000 Server 的目标计算机没有相似的硬件，就可以使用 Syspart 方法。 这种方法去掉了安装的文件复制阶段，从而减少了部署时间。

Syspart 要求使用两个物理磁盘，其中在目标硬盘上要有主分区。

如果需要安装的硬件类型的 HAL 或大型存储设备控制器不同，要进行相似的安装和操作系统配置，可以使用 Syspart 创建一组主控文件，让它们包括要映射的必要配置信息和驱动程序支持。这些映射将保证在不同的系统正确检测硬件，并一致地配置基础操作系统。如果环境包含多种“硬件-依赖”型的系统，可以使用 Syspart 为每种类型分别创建主控。请先在每种类型的一台计算机上安装 Windows 2000 ，然后使用 Sysprep 为其余计算机创建映射。有关 Sysprep 的更多信息，请参见本章后面的“使用 Sysprep 复制磁盘”。

在开始这一过程之前，请选择一台计算机作为参照。参照计算机必须安装了 Windows NT 或 Windows 2000。

要使用 Syspart 安装 Windows 2000 Server，请

1. 启动参照计算机并连接到分发文件夹。
2. 运行安装程序。

   单击“开始”，单击“运行”，然后键入：

   ```
   winnt32 /unattend:unattend.txt /s:install_source
   /syspart:second_drive /tempdrive:second_drive/ noreboot
   ```

   重要提示 为了成功完成 Syspart 安装，必须使用 /tempdrive 参数。当使用 **/**tempdrive 命令行开关时，要保证在第二分区上有足够的可用磁盘空间以安装 Windows 2000 Server 和应用程序。作为 Syspart 目标的磁盘几何结构必须和复制目标磁盘的几何结构相同。

   注意 */syspart* 和 */tempdrive* 参数必须指向副硬盘的同一分区。Windows 2000 Server 的安装必须在副硬盘的主分区上进行。

   警告 Syspart 将自动把驱动器标记为活动的默认启动设备。因此，再次启动计算机之前，请先删除该驱动器。

   相关的定义包括：

   Unattend.txt。用于无人参与安装的应答文件。它代替最终用户，提供了在安装过程中需要的应答信息。创建主映射时，可以选择是否使用应答文件。

   install_source.Windows 2000 Server 文件的位置。如果想同时从多个源进行安装，请指定多个 **/s** 命令行开关。

   second_drive.预装 Windows 2000 和应用程序的可选副驱动器。

使用 Sysprep 复制磁盘

如果需要在多台计算机上安装相同的配置，磁盘复制是一个很好的选择。在主控计算机上，安装 Windows 2000 及希望安装在目标计算机上的任何应用程序。然后运行 Sysprep 和第三方磁盘映射工具。Sysprep 会在主控计算机上准备硬盘，以便磁盘映射工具可以把硬盘的映像传输到其它计算机上。与标准安装和脚本安装相比，这种方法可以减少大量的部署时间。

要使用 Sysprep，主控计算机和目标计算机必须有相同的 HAL、高级配置和电源接口 (ACPI) 支持、以及大型存储设备控制器。 Windows 2000 会自动检测即插即用设备，当运行 Sysprep 之后再开机时，Sysprep 会重新检测并列出系统设备。这就是说，主控计算机和目标计算机上的即插即用设备，如网卡、调制解调器、视频适配器和声卡可以不必相同。Sysprep 安装的主要优势在于速度。映像可以打包并压缩，并且只有特定配置需要的文件才作为映像的一部分创建。同时，有可能其它系统上需要的其它即插即用驱动程序也被创建。映像也可以复制到 CD 上，然后分发到链接速度缓慢的远程站点。

备注 由于要求主控和目标计算机有相同的 HAL、ACPI 支持以及大型存储设备控制器，可能需要做多个映像。

Sysprep 允许您先配置一个主映像包含成员服务器所需组件，然后配置服务器，同时可以选择将其提升为域控制器。这可以手动实现，也可以通过在 Sysprep.inf 的 [GuiRunOnce] 段中运行一些命令实现。有关 Sysprep.inf 的更多信息，请参见本章后面的“使用 Sysprep 复制磁盘”。

重要提示 执行磁盘复制时，请与软件供应商核实不会违反复制软件的安装许可协议。

Sysprep 过程概述

本节描述了建立源计算机，以进行磁盘复制的过程。

1. 安装 Windows 2000 —— 在与目标计算机有相似硬件的计算机上安装 Windows 2000 Server。建立计算机的不能将加入域，并且必须把本地管理密码留为空白。

2. 配置计算机 —— 以管理员方式登录，然后安装并自定义 Windows 2000 Server 及相关应用程序。还可以加入 Internet 信息服务 (IIS) 或设置其它服务。

3. 使映射生效 —— 按您定义的准则运行审核，以校验映射配置正确。删除残留信息，包括审核和事件日志遗留的任何信息。

4. 为复制准备映射 —— 在确信计算机完全按您的意图配置以后，就可以为复制准备系统了。这可以用可选文件 Sysprep.inf 运行 Sysprep 完成，在本章后面进行说明。Sysprep 完成后，计算机会自动关机或显示可以安全关机。

5. 复制 —— 在这一点，计算机硬盘被触发运行即插即用检测，创建新的安全识别器 (SID)，然后在系统下次启动时运行“小型安装向导”。现在已经做好了使用硬件或软件方案复制或映射系统的准备。Windows 2000 Server 下次从该硬盘启动，或是从任何由该映射建立的复制硬盘上启动时，系统会检测并重新列出即插即用设备，以完成目标计算机的安装和配置。

   重要提示 依赖 Active Directory 的组件不能被复制。

Sysprep 文件

要使用 Sysprep，可以手动运行 Sysprep.exe，也可以通过使用应答文件的 [GuiRunOnce] 段配置安装程序自动运行 Sysprep.exe。为了运行 Sysprep，Sysprep.exe 和 Setupcl.exe 文件必须位于系统驱动器根目录下 (%systemdrive%\Sysprep\) 的 Sysprep 文件夹中 。要在自动安装过程中把文件放到正确的位置，必须把这些文件添加到 OEM\$1\Sysprep\ 子文件夹下的分发文件夹。有关该子文件夹的更多信息，请参见本章后面的“构建分发文件夹”。

这些文件会在复制和启动“小型安装向导”之前准备操作系统。您也可以将可选应答文件 Sysprep.inf 加入 Sysprep 文件夹。Sysprep.inf 包含了一些默认参数，可用来在合适位置提供一致的响应。这一点可以减少对用户输入的要求，从而减少了潜在的用户错误。也可以把 Sysprep.inf 文件放到软盘上，在 Windows 启动屏幕出现后将其放进软盘驱动器，以进一步自定义目标计算机。当“小型安装向导”“请稍候”屏幕出现时，就开始读取软盘驱动器。“小型安装向导”成功完成任务以后，系统最后一次重新启动，Sysprep 文件夹及其中所有内容将被删除，系统为用户登录作好准备。

Sysprep.exe

Sysprep.exe 有三个可选参数：

- *quiet* — 运行 Sysprep 时不显示屏幕消息。
- *nosidgen* — 运行 Sysprep 时不再生成系统已有的 SID。如果不准备复制运行 Sysprep 的计算机，这一参数很有用。
- *reboot* -- Sysprep 关闭计算机后，自动重新启动，使您不必再手动开机。

Sysprep.inf

Sysprep.inf 是使小型安装过程自动化的应答文件。它使用与安装程序应答文件同样的 .ini 文件语法和关键字名称（为所支持的关键字）。要把 Sysprep.inf 文件放在 %systemdrive%\Sysprep 文件夹中或软盘上。如果使用软盘，可以在 Windows 启动屏幕出现后提交软盘。“小型安装向导”“请稍候”屏幕出现时，开始读取软盘驱动器。注意，如果运行 Sysprep 时不加入 Sysprep.inf,“小型安装向导”会显示所有可用的对话框，本章后面“使用 Sysprep 复制磁盘”中列出了这些对话框。

备注 如果您在主控计算机上提供 Sysprep.inf 文件，并想对每台计算机都分别更改 Sysprep.inf，可以使用以前讨论过的软盘方法。

以下是 Sysprep.inf 文件的一个示例：

```
[Unattended]
;Prompt the user to accept the EULA.
OemSkipEula=No
;Use Sysprep's default and regenerate the page file for the system
;to accommodate potential differences in available RAM.
KeepPageFile=0
;Provide the location for additional language support files that
;might be needed in a global organization.
InstallFilesPath=%systemdrive%\Sysprep\i386

[GuiUnattended]
;Specify a non-null administrator password.
;Any password supplied here will only take effect if the original
source
;for the image (master computer) specified a non-null password.
;Otherwise, the password used on the master computer will be
;the password used on this computer. This can only be changed by
;logging on as Local Administrator and manually changing the password.
AdminPassword=""
;Set the time zone
TimeZone=20
;Skip the Welcome screen when the system boots.
OemSkipWelcome=1
;Do not skip the regional options dialog box so that the user can
;indicate which regional options apply to them.
OemSkipRegional=0

[UserData]
;Prepopulate user information for the system.
FullName="Authorized User"
OrgName="Organization Name"
ComputerName=XYZ_Computer1

[GUIRunOnce]
;Promote this computer to a Domain Controller on reboot.
DCPromo/answer:<location of dc promo answer file>

[Identification]
;Join the computer to the domain ITDOMAIN
JoinDomain=ITDOMAIN

[Networking]
;Bind the default protocols and services to the network card(s) used
;in this computer.
InstallDefaultComponents=Yes
```

备注 只有当当前管理密码为空时，才能用 Sysprep.inf 更改管理密码。在 Sysprep GUI 阶段更改管理员密码时也是同样道理。

有关 Sysprep.inf 使用的应答文件段及命令的更多信息，请参见本书附录“无人参与安装应答文件示例”。

Setupcl.exe

Setupcl.exe 可以完成以下任务：

- 为计算机再生新的安全 ID 。
- 启动小型安装向导。

小型安装向导

当计算机从用 Sysprep 方法复制的磁盘上首次启动时，“ 小型安装向导 ”启动 。该向导会收集进一步自定义目标计算机所需要的任何信息。如果不使用 Sysprep.inf，或把该文件的某些段留为空白，“ 小型安装向导 ”会出现屏幕显示哪些段在 Sysprep.inf 中没有提供应答。可能的屏幕显示包括：

- 最终用户许可协议 (EULA)
- 区域选项
- 用户名和公司
- 计算机名和管理员密码
- 网络设置
- TAPI 设置（只有当计算机上有调制解调器或新的调制解调器设备时显示）
- 服务器授权（只对服务器）
- 时区选择
- 完成/重新启动

如果想绕过这些屏幕，可以在 Sysprep.inf 中指定某些参数。表 13.6 中列出了这些参数。

备注 由于安装程序已经为显示设备检测了最佳设置，当安装程序或者小型安装向导运行时您就看不到“ 显示设置 ”了。可以在主控计算机使用的应答文件中，或在目标计算机使用的 Sysprep.inf 文件中指定 [Display] 设置。如果 [Display] 设置放在主控计算机使用的应答文件中，Sysprep 会保持这些设置，除非 Sysprep.inf 包含其它设置，或者视频适配器或监视器要求的设置与主控计算机所检测的不同。

表 13.6 绕过小型安装向导所需的 Sysprep.inf 中的参数

参数	值
区域选项	[RegionalSettings] ;Section [GuiUnattended] OemSkipRegional=1
用户名和公司	[UserData] FullName="User Name" OrgName="Organization Name"
计算机名和管理员密码	[UserData] ComputerName=W2B32054 [GuiUnattended] AdminPassword=""
网络设置	[Networking] InstallDefaultComponents=Yes

TAPI 设置	[TapiLocation] AreaCode=425
时区选择	[GuiUnattended] TimeZone=<desired time zone index>
完成/重新启动	NA

手动运行 Sysprep

安装 Windows 2000 Server 以后，可以用 Sysprep 准备系统，以将系统传送到配置类似的其它计算机。为了手动运行 Sysprep ，首先必须安装 Windows 2000 Server，配置系统并安装应用程序。然后不使用 *–reboot* 命令行开关运行 Sysprep 。系统关闭后，把驱动器映像复制到有类似配置的计算机上。

当用户首次启动复制的计算机时，Sysprep 小型安装程序运行，并允许用户自定义其系统。也可以用 Sysprep.inf 预先指定 Sysprep 配置的部分或全部参数。Sysprep 小型安装程序完成后，Sysprep 文件夹（包括 Sysprep.exe 和 Setupcl.exe）被自动删除。

要为复制准备 Windows 2000 Server 安装，请

1. 在“开始”菜单上，单击“运行”，然后键入：

   cmd

2. 在命令提示符下，更换到 C 驱动器的根文件夹，然后键入：

   md sysprep

3. 载入 Windows 2000 Server CD。打开 \Support\Tools 文件夹中的 Deploy.cab 文件。

4. 将 Sysprep.exe 和 Setupcl.exe 复制到 Sysprep 文件夹。

   如果正在使用 Sysprep.inf，也要把它复制到 Sysprep 文件夹。注意 Sysprep.exe、Setupcl.exe 和 Sysprep.inf 必须在同一个文件夹中，以便 Sysprep 可以正常运行。

5. 在命令提示符下，切换到 Sysprep 文件夹：

   cd sysprep

6. 根据需要，键入以下内容：

   Sysprep
   Sysprep –reboot
   Sysprep */<optional parameter>*
   Sysprep */<optional parameter>* -reboot
   Sysprep */<optional parameter 1>*U/*<optional parameter X>*
   Sysprep */<optional parameter 1>*U/*<optional parameter X>* -reboot

7. 如果没有指定 –reboot 命令行开关，请执行以下操作：

   当有消息出现提示关闭计算机时，在“开始”菜单处单击“关闭系统”。现在，已经准备好使用第三方磁盘映射工具创建安装的映像了。

   如果指定 –reboot 命令行开关只用于审核目的，则计算机会重新启动而且小型安装向导运行。在这种情况下，请进行如下操作：

   - 校验小型安装向导提供了所需的提示。这时也可以审核系统和其它应用程序。审核一旦结束，不使用 –reboot 命令行开关再次运行 Sysprep。

- 当有消息出现提示关机时，请在“开始”菜单处单击“关闭系统”。现在，已准备好使用第三方磁盘映射工具创建安装的映像了。

备注 可以把一个 Cmdlines.txt 文件加入安装程序将要处理的 Sysprep 文件夹。该文件将运行安装程序以后的命令，包括安装应用程序所需的命令。

在安装结束后自动运行 Sysprep

应答文件的 [GuiRunOnce] 段包含了要在安装程序结束后执行的一些命令。您可以使用 [GuiRunOnce] 段创建安装以完成安装程序、自动登录到计算机、以 **–quiet** 模式运行 Sysprep ，然后关闭计算机。要出现这种情况，需要做以下事情：

1. 将需要的 Sysprep 文件加入 OEM\$1\Sysprep\ 下的分发文件夹，以把文件复制到系统驱动器的正确位置。
2. 在应答文件的 [GuiRunOnce] 段，将以下命令作为在计算机上最后运行的命令：

   ```
   %systemdrive%\Sysprep\Sysprep.exe –quiet
   ```

   如果需要多次重新启动，请将此作为最后一次使用 [GuiRunOnce] 段时最后用到的命令。

使用 Sysprep 扩展磁盘分区

使用 Windows 2000 GUI 安装程序和小型安装程序，可以通过应答文件扩展 NTFS 分区。这一新功能可以完成以下任务：

- 使您可以创建可扩展成更大磁盘分区的映像，以便充分利用可能比主控计算机的原始硬盘空间更多的硬盘。
- 提供了可以在较小的硬盘上创建映射的方法。

为了确定将该功能集成到环境的最好途径，需要检查以下步骤，并根据映射操作系统的工具选择一种最好的方法。

警告 如果映射工具可以编辑映像，可以删除 Pagefile.sys、Setupapi.log 和 Hyberfil.sys（如果有的话），因为当目标计算机运行小型安装向导时，这些文件都将被重建。您不能在活动系统上删除这些文件，因为这将导致系统不能正常运行。如做了要求，这些文件只能从映像中删除。

要使用第三方映射产品或支持 Windows 2000 使用的 NTFS 的硬件映射设备扩展硬盘分区，请

1. 配置主控计算机的硬盘分区，使其具有安装 Windows 2000 所有组件和计划预装的应用程序所需的最小空间。这可以减少总的映像大小需求。
2. 在用于创建主映像的应答文件 [Unattended] 段中加入 FileSystem=ConvertNTFS。由于想保留最小的映像可能大小，则没必要在此加入 ExtendOemPartition。

   备注 ConvertNTFS 在 Sysprep.inf 中无效，因为这是一个只对文本模式功能，而 Sysprep 无法进入文本模式。
3. 在 Sysprep.inf 的 [Unattended] 段加入如下语句：

   ```
   ExtendOemPartition = 1
   ```

   （或以 MB 为单位的附加大小，以扩展分区）
4. 在主控计算机上安装 Windows 2000。Sysprep 将自动关闭系统。

5. 映射驱动器。
6. 把映像放到目标计算机上，目标计算机系统分区与主控计算机大小相同。
7. 重新启动目标计算机。

   小型安装向导启动，并立即扩展分区。

要使用不支持 Windows 2000 使用的 NTFS 的映射产品扩展硬盘分区，请

1. 配置主控计算机上的硬盘分区，使其具有安装 Windows 2000 所有组件及计划预装的应用程序所需的最小空间。这可以减少总的映像大小要求。
2. 使用 Windows 2000 提供的 Convert.exe 工具把文件系统转换成 NTFS。
3. 在用于创建主控映像的应答文件中加入以下内容，作为 [GuiRunOnce] 段的最后两项：

   ```
   [GuiRunOnce]
   <Command1> = "<command line>"
   <Command2> = "<command line>"
   ...
   <Commandn-1> = "Convert c:\ /fs:ntfs"
   <Commandn> = "%systemdrive%\sysprep\sysprep.exe -quiet"
   ```

   这里：

   - <command line> 包括安装应用程序或配置操作系统需要运行的任何命令。
   - <Commandn-1> 是应答文件 [GuiRunOnce] 段中倒数第二个执行的命令。它会运行 **convert** 命令。由于 **convert** 命令无法在操作系统运行时把活动系统转换成 NTFS，所以操作系统设置为在下次重新启动时转换系统。由于 Sysprep 是下一个要运行的项，所以在此过程中系统不会转换成 NTFS。
   - <Commandn> 是计算机最后运行的一个命令。它应该是 Sysprep.exe。Sysprep 运行时，该命令先为映射准备计算机，然后关闭计算机。

   备注 在这一步，不能把 ExtendOemPartition 加入主应答文件，因为映像生成的分区不是 NTFS。一般可能希望映像尽可能得小。
4. 请在 Sysprep.inf 的 [Unattended] 段加入以下语句：

   ```
   ExtendOemPartition = 1
   ```

   （或以 MB 为单位的附加大小，以便扩展分区）
5. 在主控计算机上安装 Windows 2000。Sysprep 将自动关闭系统。

   重要提示 不要重新启动计算机。
6. 映射驱动器。
7. 把映像放到目标计算机上，目标计算机有与主控计算机相同大小的系统分区。
8. 重新启动目标计算机。

   计算机最初以转换模式启动，以把目标计算机的系统分区转换成 NTFS。

   计算机将自动重新启动。

小型安装向导启动，并立即扩展分区。

使用 Systems Management Server

您可以使用 SMS 执行 Windows 2000 Server 对多个系统的升级管理，特别是在这些系统地点分散时。注意只有计算机上有以前安装的操作系统时，才可以用 SMS 安装。使用 SMS 升级之前，请先评估现有的网络基本配置，包括带宽、硬件和地理限制，这非常重要。使用 SMS 升级的主要好处在于您可以对升级过程集中控制。例如，您可以控制升级什么时候进行（比如在培训过程中或培训之后、硬件检查以后或用户数据备份以后），哪些计算机将被升级，以及如何应用网络约束。有关 SMS 部署的更多信息，请参见本书中的“使用 Systems Management Server 部署 Windows 2000”。

使用可引导光盘

在那些基本输入/输出系统（BIOS）允许从 CD 启动的计算机上，可以使用可引导 CD 方法安装 Windows 2000 Server。这种方法对连接速度较慢、没有本地 IT 部门的远程站点上的计算机非常有用。可引导 CD 方法将运行 Winnt32.exe，而它可以进行快速安装。

备注 可引导 CD 方法只能用于全新安装。为了进行升级，必须从现有的操作系统中运行 Winnt32.exe。

为了保证最大程度的灵活性，请把 BIOS 的启动顺序设置如下：

- 网卡
- CD
- 硬盘
- 软盘

要使用可引导 CD，必须满足以下条件：

- 计算机必须具有对可引导的 CD 的 El Torito No Emulation 支持。
- 应答文件必须包含有所需关键字的 [Data] 段。
- 应答文件必须命名为 Winnt.sif，并放在软盘上。

有关应答文件参数和语法的更多信息，请参见 Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，请使用 Windows “资源管理器”访问该文件。在 Windows 95 及早期版本，或从 MS-DOS 中，请使用 **Extract** 命令访问该文件。

要使用可引导光盘安装 Windows 2000 Server，请

1. 从 Windows 2000 Server CD 上启动系统。
2. 当“Windows 2000 安装程序”蓝色文本模式屏幕出现时，把包含 Winnt.sif 文件的软盘放入软盘驱动器。
3. 一旦计算机从软盘驱动器读取，移走软盘。安装程序这时按 Winnt.sif 文件的指定从 CD 运行。

备注 可引导 CD 的方法要求所有必需的文件都在 CD 上。唯一性数据库文件 (UDB) 不能应用这种方法。

安装配置示例

以下示例包括了如何在已有服务器配置或尚无配置的计算机上安装 Windows 2000 Server 程序。

现有服务器

这部分的示例适用于已经有以下服务器配置的计算机：

- 运行 Windows NT Server 并有 Windows 2000 Server 兼容服务器应用程序的计算机。
- 运行 Microsoft® Windows NT® Server 3.5 或更早版本的计算机，或运行非 Microsoft 操作系统的服务器。

例 1：Windows NT Server 与 Windows 2000 兼容服务器应用程序

本示例给出了在有或没有兼容硬件、运行 Windows NT Server 的计算机上安装 Windows 2000 Server 的两种方法。

要在有兼容硬件的计算机上安装 Windows 2000 Server，请

1. 备份整个系统。

   用以下方法之一升级系统：

   - 初始化“推”安装。意思是程序或应用程序被从主控计算机自动发送到目标计算机。这种方法不需要用户或管理员初始化该活动。

     – 或 –

   - 通过从命令提示以选中的参数运行 Winnt32.exe，初始化本地安装。

     – 或 –

   - 执行手动安装（无应答文件），然后应答所有提示。

     – 或 –

   - 执行自动或半自动安装。在完全自动安装中，应答文件为所有问题提供应答。半自动安装允许您确定自动程度，并让用户为某些应用程序输入信息。

要在有不兼容硬件且不需要替换硬盘的计算机上安装 Windows 2000 Server，请

1. 更换除硬盘以外的所有必须的硬件。
2. 验证所有新硬件运行正常。
3. 备份整个系统。

   请用以下方法之一升级系统：

   - 初始化“推”（全自动）安装。

– 或 –

- 通过从命令提示以选择的参数运行 Winnt32.exe，初始化本地安装。

– 或 –

- 执行手动安装（无应答文件），然后应答所有提示。

– 或 –

- 执行自动或半自动安装。

要在有不兼容硬件且需要更换硬盘的计算机上安装 Windows 2000 Server，请

升级下列组件中的一个或全部：

- RAM
- 处理器

2. 验证所有新硬件运行正常。
3. 备份整个系统。
4. 更换硬盘。复制备份的映像。

   如果进行的是升级，请使用下列方法中的一种。这在服务器处于唯一或接近唯一配置的情况下，尤其适用：

   - 初始化“推”（全自动）安装。

     – 或 –

   - 通过从命令提示以选择的参数运行 Winnt32.exe，初始化本地安装。

     – 或 –

   - 执行手动安装（无应答文件），然后应答所有提示。

     – 或 –

   - 执行自动或半自动安装。

   如果进行的是全新安装，请使用下列方法中的一种。

   - 在用磁盘复制硬件或软件更换硬盘之前，先用 Syspart 方法把所有需要的文件放在硬盘上。系统启动时，安装程序会自动运行。重新安装所有必要的服务器应用程序程序。

     – 或 –

   - 初始化“推”（全自动）安装。

     – 或 –

   - 通过从命令提示以选择的参数运行 Winnt32.exe，初始化本地安装。

     – 或 –

   - 执行手动安装（无应答文件），然后应答所有提示。

– 或 –

- 执行自动或半自动安装。

例 2：运行 Windows NT Server 3.5 或更早版本的计算机，或运行非 Microsoft 操作系统的服务器

无法直接升级为 Windows 2000 Server 的服务器操作系统包括：Windows NT 3.5 或更早版本、Novell、 Banyan Vines、UNIX 和 OS/2。为了准备全新安装，请首先获取由 OEM 或解决方案提供商生产的客户计算机。

要在运行 Windows NT 3.5 或更早版本或非 Microsoft 操作系统的计算机上安装 Windows 2000，请

1. 备份整个系统。

   用下列方法之一，从命令提示以希望的参数运行 Winnt.exe：

   - 执行手动安装（无应答文件），然后应答所有提示。

   – 或 –

   执行自动或半自动安装。请使用下列方法中的一种：

   - CD 引导安装程序。
   - Syspart 方法。这在计算机上安装新硬盘时很有用。
   - Sysprep 方法。在相同的计算机（ HAL 和大型存储设备控制器必须相同）上安装时使用。

   备注 如有必要，可以在在现有的计算机上执行全新安装，但不推荐这样做。如果服务器无法升级，可以将每台服务器用包含 Windows 2000 Server 全新安装的新服务器代替。您必须这样做，以确保系统能够长时间稳定，减少潜在对用户的影响，并确保有时间将必要的索引和设置迁移到新服务器上。

2. 安装与 Windows 2000 Server 兼容的应用程序。
3. 验证系统按要求运行。
4. 在关闭现有系统之前，请把用户和索引迁移，以指向新系统。

新服务器

对尚未安装 Windows 2000 以前版本操作系统的计算机，需要进行 Windows 2000 Server 的全新安装。

为了准备安装，请先取得由 OEM /解决方案提供商生产的计算机。

要在尚未安装 Windows 2000 以前版本操作系统的计算机上安装 Windows 2000 Server，请;

1. 执行手动安装（无应答文件）。应答所有提示。

   – 或 –

   执行自动或半自动安装。请使用下列方法中的一种：

- CD 引导安装程序。
- Syspart 方法。这在计算机上安装新硬盘时很有用。
- Sysprep 方法。在相同的计算机（ HAL 和大型存储设备控制器必须相同）上安装时使用。
- 启动磁盘并使用应答文件运行安装程序。

安装规划任务列表

表 13.7 是安装 Windows 2000 Server 和所需的应用程序时涉及的主要任务的摘要。

表 13.7 安装任务摘要

任务	章节中的位置
解决关键规划问题	解决关键规划问题
创建分发文件夹。	准备安装
检查应答文件	检查应答文件
检查 Windows 2000 安装命令	准备安装
基于关键规划选择应用程序安装方法。	服务器应用程序自动安装
基于关键规划选择操作安装方法。	Windows 2000 Server 自动安装

第 14 章 – 使用 Systems Management Server 部署 Windows 2000

Microsoft® Systems Management Server (SMS) 提供了多种工具，帮助您在企业环境下部署 Microsoft® Windows 2000 Server 和 Microsoft® Windows 2000 Professional。与此过程相关的项目负责人和分析员、Windows 2000 技术分析员和 SMS 管理员都应该熟悉本章描述的推荐配置和程序。尽管这些建议也适用于较小的单位，但它们主要针对的是有 2,500 台以上个人计算机的较大单位。

理解本章信息并不需要熟悉 Systems Management Server 2.0 版。但要进行 Windows 2000 部署，就需要 SMS 方面的专家。本章假定您的 SMS 基础结构已经建好，或者会在部署 Windows 2000 前建好。本章还描述了 SMS 2.0 和 Systems Management Server 1.2 版的重要区别。

本章内容

使用 Systems Management Server 分发软件
为 Systems Management Server 封装 Windows 2000
分发 Windows 2000 程序包
公布 Windows 2000 程序包
使用 Systems Management Server 简化域合并和域迁移
比较 Systems Management Server 1.2 与 Systems Management Server 2.0 之间的区别
为使用 Systems Management Server 部署 Windows 2000 规划任务列表

本章目标

本章将帮助您创建以下规划文档：

- Windows 2000 软件分发规划。
- Windows 2000 SMS 程序包定义。

资源工具包中的相关信息

- 有关 Windows 2000 自动升级的更多信息，请参见本书的“服务器自动安装与升级”和“客户自动安装与升级”。
- 有关自动域合并和域迁移的更多信息，请参见本书的“确定域迁移策略”。

使用 Systems Management Server 分发软件

使用自动安装会使部署 Windows 2000 大大简化。但在将自动程序应用到单位中多个服务器和客户计算机时，还是会涉及许多任务。这些任务包括：

- 选择为 Windows 2000 配备及做好了支持准备的计算机。
- 将 Windows 2000 源文件分发到所有站点，包括远程站点和没有技术人员支持的站点。
- 监视到所有站点的分发。
- 安全地为升级提供足够的操作系统权限。
- 自动初始化程序包安装，并让用户可以控制安装时间。
- 解决与分发或安装相关的问题。

- 报告部署速率和成功情况。

Systems Management Server 可以帮助您完成所有这些任务。图 14.1 中图示说明了用 SMS 部署 Windows 2000 涉及的主要任务。

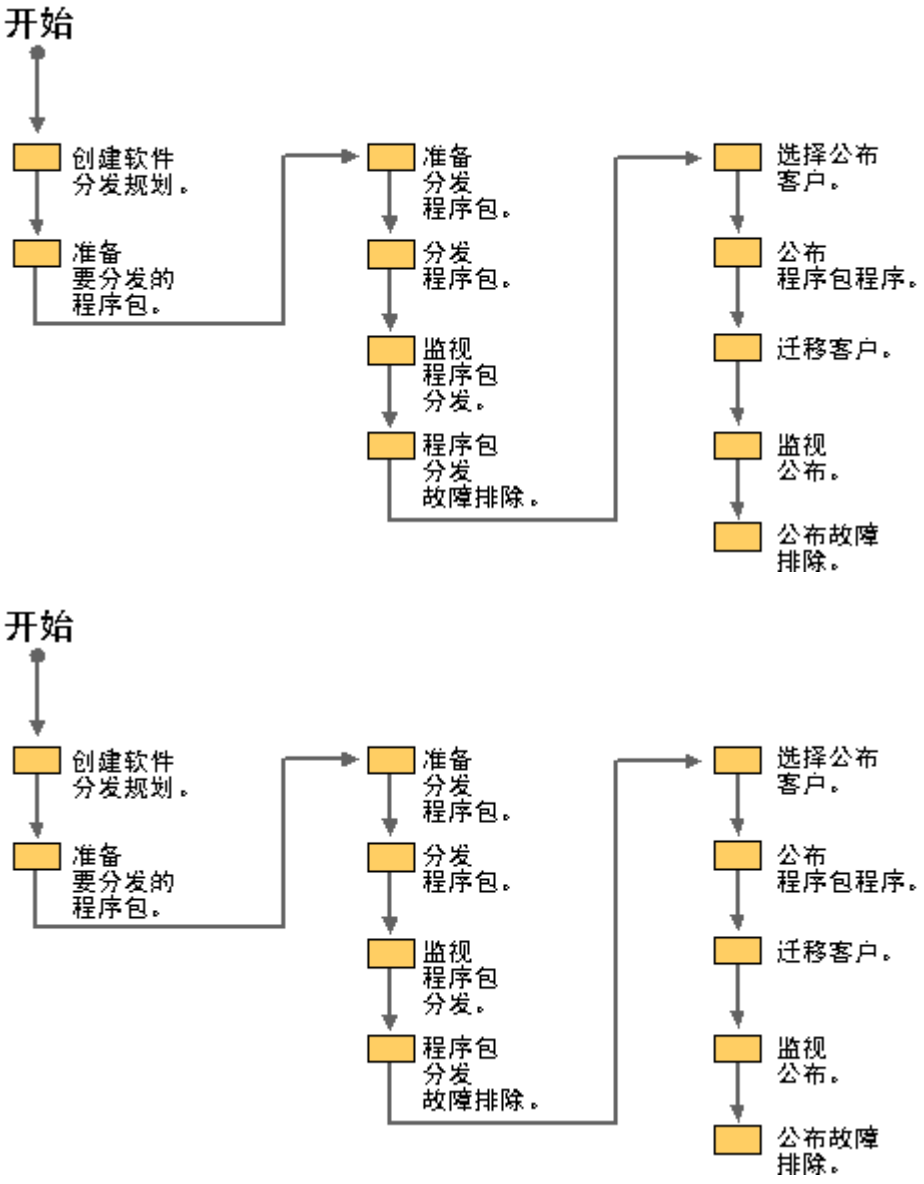


图 14.1 用 SMS 部署 Windows 2000

SMS 为现有计算机的升级提供了工具，但没有为没有安装操作系统的新计算机安装提供工具。要使用 SMS 软件分发，必须在目标计算机上安装 SMS 客户组件。这些 SMS 组件要求计算机配置适当的操作系统。

备注 “SMS 客户”指所有目标计算机而不考虑其功能。

但您可以用当前的 SMS 客户将 Windows 2000 初始化安装到新的目录层次或磁盘分区。这种情况下，Windows 2000 安装将是一个全新安装而不是升级。

备注 您也可以使用 SMS 进行其它 Windows 2000 部署活动。有关在 Windows 2000 部署中使用 SMS 的详细信息，请参见本书的“使用 Systems Management Server 分析网络基础结构”。

使用 Systems Management Server 2.0 进行软件分发

Systems Management Server 软件分发基于多个组件和任务，可以让您完全控制分发过程。

SMS 程序包

SMS 软件分发从“ SMS 程序包 ”开始。程序包是软件分发的基本单位，包含了程序源文件和指引软件分发过程的详细信息。

每个程序包至少包含一个“ 程序 ”，该“ 程序 ”是一命令行，在各目标计算机上运行，控制程序包的执行。程序可以指引软件的安装，也可以包含要在各目标计算机运行的任何其它命令行。大部分程序包还包含“ 程序包源文件 ”，如软件安装文件，它们会在程序运行时用到。

一些软件应用程序提供了扩展安装选项。另一些程序包和工具则不提供这些选项。如果想要分发的程序没有提供合适的安装选项，如无人参与运行，您可以使用 SMS 安装服务为软件分发做好程序准备。SMS 安装服务可以生成能够完全自定义的参与安装和无人参与安装脚本。这种脚本不适于 Windows 2000 升级。但它对 Windows 2000 升级前为准备计算机而发送的程序包，或升级后为完成配置而发送的程序包可能有用。有关 SMS 安装服务的更多信息，请参见 *Microsoft ® Systems Management Server Administrator's Guide* 中的“ Creating Self-Extracting Files with SMS Installer 2.0 ”。

您可以使用 SMS 管理员控制台中的“ 程序包 ”创建程序包，也可以通过创建或获取一个程序包定义文件，使用“ 从定义创建程序包 ”向导创建程序包。程序包定义文件是创建程序包的一种非交互式替代方法。它是一个包含创建程序包所有必需信息的格式化文件。SMS 2.0 中就包含了一个 Windows 2000 的程序包定义文件。您可以用 SMS 工具和向导从程序包定义文件创建程序包，而无需用户的干预。程序包创建后，请使用 SMS“ 管理分发点 ”向导选择分发点。

分发

程序包也包含了软件分发的信息，如程序包源文件目录。“ 分发点 ”是站点系统的共享点，程序包源文件在这里复制，以备客户计算机访问。程序包还包括有关如何、何时更新分发点的信息。为了方便管理，可以将分发点分成“ 分发点组 ”。

当程序包文件需要传播到其它站点时，SMS 会压缩这些文件以便在站点间传送。您也可以在源站点内创建并使用程序包源文件的压缩备份。

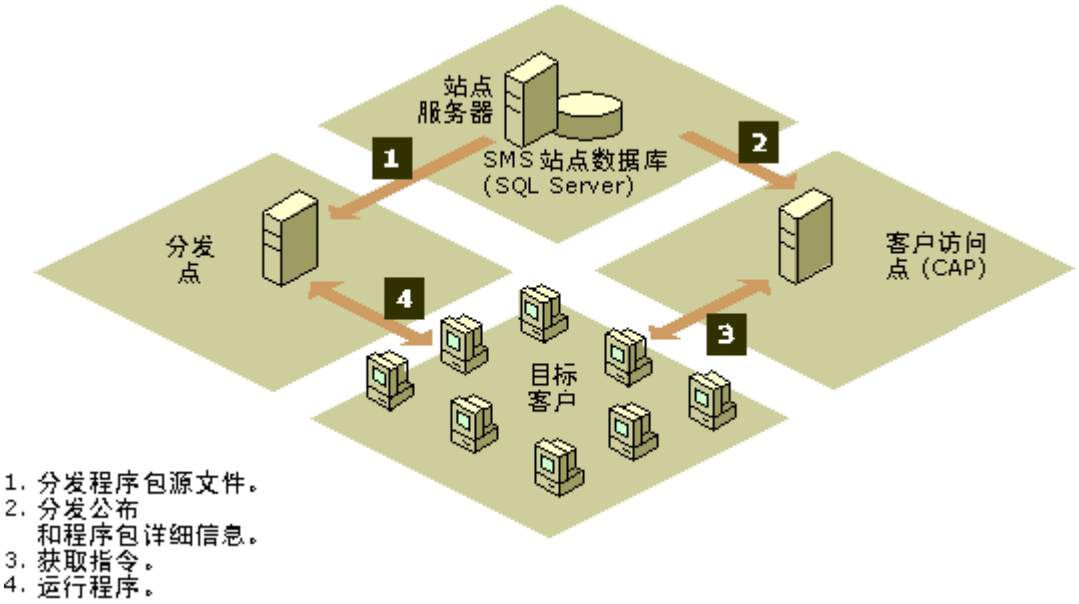
您可以使用“ 分发点 ”控制程序包的分发，“ 分发点 ”位于 SMS 管理员控制台中“ 程序包 ”下的程序包定义之下。

公布

创建 Windows 2000 程序包后，就可以通过创建公布向用户公布程序包中的一个或多个程序。公布会指定什么程序对客户计算机可用，哪些计算机会接收到该公布，以及计划何时安装程序。图 14.2 显示了软件分发的过程。

SMS 客户接收到公布之后，用户还可以在一定程度上控制程序包的时间安排。公布可以在特定的特权模式下运行，这样就无需将特权授予用户。您也可以运行公布让它的操作不受用户的干预。

请使用 SMS 管理员控制台中的“ 公布 ”创建公布。



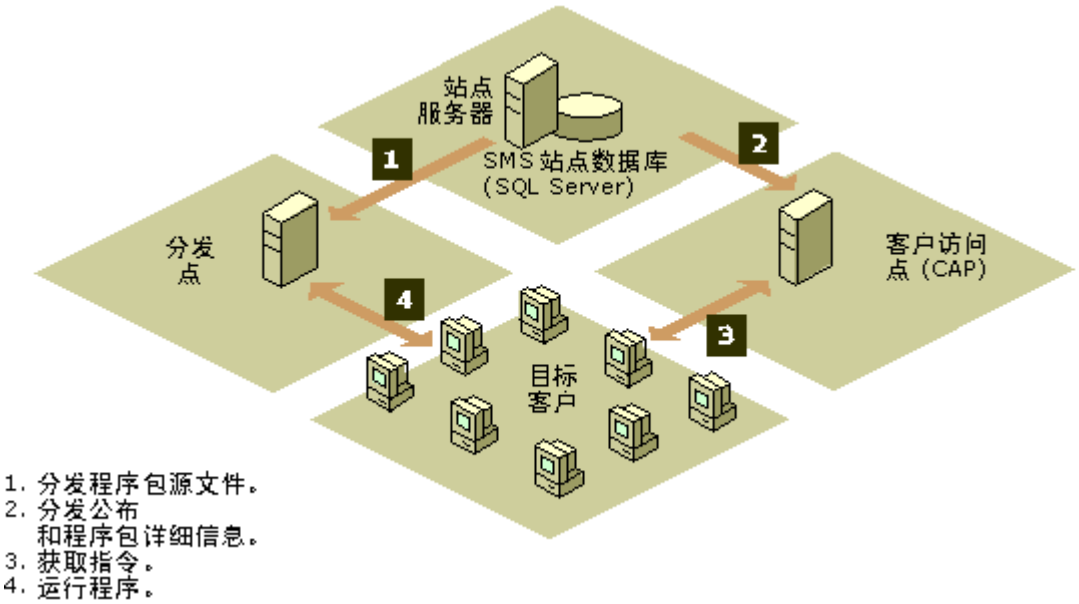


图 14.2 SMS 2.0 软件分发流程

有关 SMS 软件分发的更多信息，请参见 *Systems Management Server Administrator's Guide*。

SMS 软件分发最佳做法

对于大型软件如 Windows 2000 的分发，有必要注意 Systems Management Server 2.0 软件分发的两个阶段：分发和公布。分发会让软件接近计算机以便升级。公布则会初始化升级。对于象 Windows 2000 一类的大型程序包，分发阶段会消耗大量资源，并且会因为缺少磁盘空间而产生一系列问题。因此，要仔细规划和监视分发。分发阶段成功完成后，公布阶段就可以开始。

请先将 Windows 2000 分发到一个站点，以测试分发。程序包的初始公布也应该只发送到这一站点的客户。这样，就可以在有限范围内测试 SMS 基础结构和程序。如果信心增加和容量许可，您可以将程序包分发到更多站点，并增大公布的范围，加入更多的客户和站点，直至最终加入整个单位。

在下面的对软件分发过程的讨论中，包括了其他最佳做法。

SMS 如何帮助 Windows 2000 部署

在以下方面，Systems Management Server 对部署 Windows 2000 特别有用。

将 Windows 2000 源文件发送到所有站点

SMS 发送器可以通过多种网络协议及事实上任一种网络链接发送文件。与传统文件传送方法相比，发送器提供了多项优点。它们可以：

- 只使用网络带宽的一部分，而允许其它商务功能同时继续进行。
- 只在指定时间转发程序包，如在大部分用户不使用链接的时间。
- 在文件传送过程中检查文件，一旦网络链接失败，传送将从最近的检查点继续进行，而不是从头开始。
- 选择到目标的备用路由。
- 使用 SMS 层次结构使程序包到达站点，而不是把程序包从原站点直接发送到所有站点。

使用发送器，会对远程站点特别是没有技术人员支持的远程站点大有帮助。这种情况下，您可以将 Windows 2000 软件可靠地分发到所有站点，而不会干扰其它的商务功能。

监视到所有站点的分发

完成每一步之后，SMS 都会自动发送一个状态消息，您可以用 SMS 状态子系统很容易地监视这些消息。

选择计算机

部署 Windows 2000 升级是一个大型、复杂、高配置的过程，因此需要分阶段进行。这既会包括网络活动，也包括需要的支持。另外，可能不会所有计算机都同时作好接收程序包的准备；例如，可能有些计算机的内存或磁盘空间不足。SMS 会收集计算机的清单信息，让您能创建查询，选择适当的计算机。随着信心增加，您可以增大选择的范围。

清单详细信息的集合会自动包含满足目前选择条件的所有新添加计算机。例如，我们考虑一个定义为内存在 64 MB 以上的计算机的集合。如果将 32 MB 内存添加到一台有 32 MB 内存的 SMS 客户计算机，该计算机将有资格接收 Windows 2000 升级，从而自动加入到集合中。

安全地提供足够的操作系统权利

操作系统升级会影响计算机的所有方面，因此需要终端用户有广泛的访问权限。把这么广的权限交给对计算机知识或重要公司策略和流程还没有深入了解的用户，您可能会感到犹豫。但 SMS 有特殊的特权，可以在这种情况下运行升级。

自动初始化安装

升级可以自动初始化，或由用户初始化。您可以设置该过程，这样即使涉及到用户，也无需他们在复杂的选项中作出选择。您也可以让用户选择控制时间安排，这样升级可以在客户不使用计算机时进行。

解决问题

如果升级到 Windows 2000 导致某台计算机出现问题，SMS 提供了帮助解决问题的功能。SMS 提供的状态和

清单信息可以让您从一个集中、方便的信息源——SMS 管理员控制台获得许多有关计算机的详细信息。您也可以用 SMS 远程工具远程控制计算机、传送文件或按其它方式操作计算机（条件是 SMS 客户有这些功能）。如果用户有不兼容或可能需要重新安装的应用程序，您可以用 SMS 软件分发将其自动升级或删除。

报告状态

SMS 状态消息不仅在程序包分发时生成，也会在公布和在用户计算机上安装时生成。您可以用这些状态消息报告部署的速率和成功情况。

在以下程序中描述了利用这些 SMS 功能需要的步骤。有关启用和有效利用相关 SMS 子系统的详细信息包含在 SMS 文档中。

为 Systems Management Server 封装 Windows 2000

使用 Systems Management Server 部署 Windows 2000 时，必须把 Windows 2000 文件放入 SMS 程序包。对 Windows 2000 Server 和 Windows 2000 Professional 需要创建不同的程序包。SMS 2.0 包括了 Windows 2000 Server 和 Windows 2000 Professional 的预定义程序包。可以用作创建 Windows 2000 程序包的起始点。

对于各个程序包，SMS 从分发文件夹获取文件。有关构建分发文件夹的更多信息，请参见本书的“自动服务器安装和升级”。您必须按本章所述构建分发文件夹，并加入完成升级所需的所有辅助文件，如即插即用设备驱动程序和应答文件。甚至还可以加入标准应用程序、语言包和服务包。

每个预定义 Windows 2000 SMS 程序包还包含 SMS 程序。每个程序都是为安装 Windows 2000 程序包而创建的不同选项组合。例如，默认程序可能会不受用户干预安装 Windows 2000。如果想允许有能力的用户选择选项，则需要一个额外的程序。所有这些 SMS 程序必须与现有分发文件夹中程序包的文件兼容。

准备 Windows 2000 Server 升级程序包

以下程序描述了如何为 Windows 2000 Server 设置典型的升级程序包。第一步是设置分发 Windows 2000 Server 的程序包的源文件和预定义 SMS 程序包的位置。

要创建 Windows 2000 Server SMS 程序包，请

1. 为程序包源文件设置位置。

   这一过程在本书的“自动服务器安装和升级”一章中做了描述。这里包括 Windows 2000 文件、一个应答文件和其它需要的文件。

2. 在 SMS 管理员控制台中，选择 Packages（程序包）。从 Action（操作）菜单，将鼠标指向 New（新建），然后单击 Package From Definition（从定义创建程序包），如图 14.3 所示。

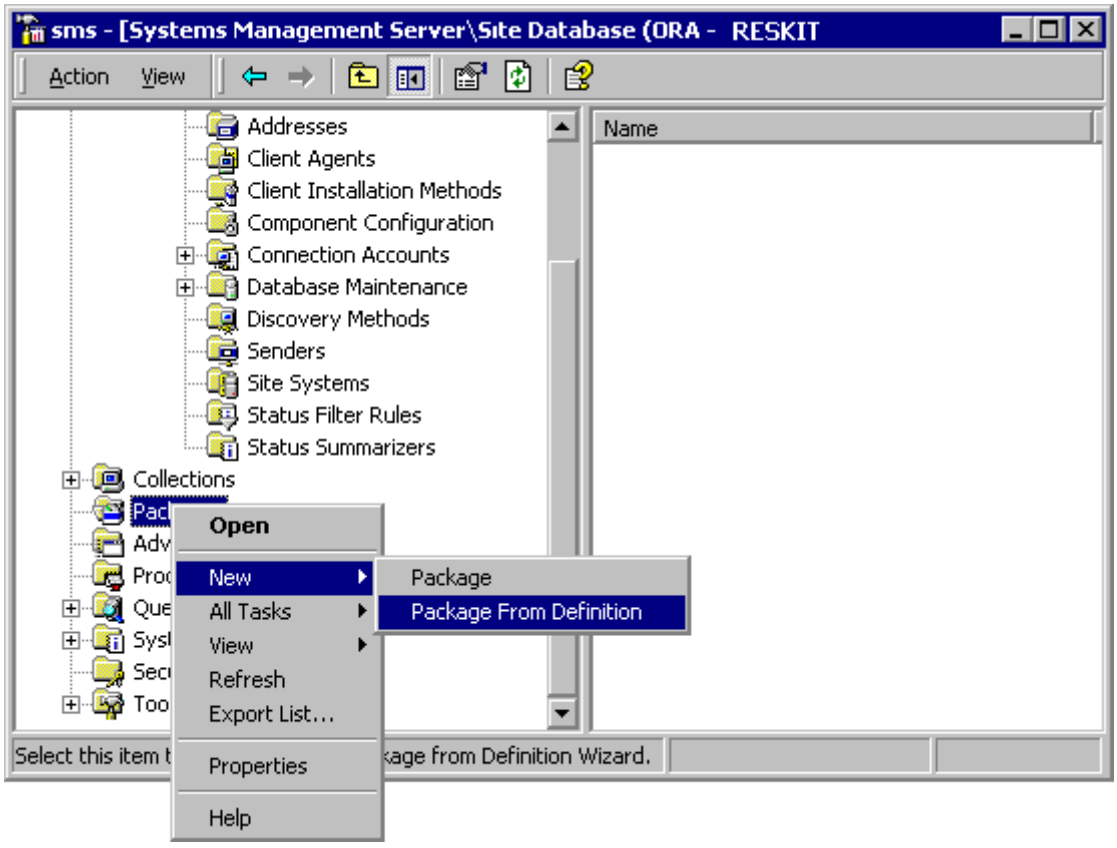


图 14.3 从定义向导初始化 SMS 程序包

3. 在欢迎页面上，单击“下一步”。从“数据包定义”列表中，单击 Windows 2000 Server。

4. 在源文件页上，单击“创建源文件的压缩版本”，然后单击“下一步”。在“源目录”框中，输入程序包源文件路径（见第 1 步）。单击“下一步”，然后单击“完成”。

   如果站点服务器的磁盘空间紧张，您可以从源文件页选择“始终从源目录获取文件”。但这样会减慢以后的软件分发速度，并要确保源目录总是可用。

5. 向导完成后，在新程序包下选择“程序”。在结果窗格（控制台右面），双击“从 NTS 3.51/4.0 (x86) 自动升级”。然后验证预定义“命令行”是需要的正确设置命令。如果还使用其它程序，请重复第 5 步。

   要验证预定义“命令行”已满足需要，请参见本章后面的“检查 Windows 2000 Server 程序包定义”。

   请考虑在程序命令行中指定应答文件，这样能够指定大量的配置选项。有关应答文件的更多信息，请参见本书的“自动服务器安装和升级”。

6. 在“注释”框，为要使用的每个程序输入一个注释。

   用户可以看到这些注释，所以要确保它们是描述性的。 同时为用户提供联系信息，如姓名、电话号码或电子邮件地址，这样用户如果需要详细信息就可以及时联系。

7. 在各程序的“要求”选项卡，把“估计磁盘空间”和“估计运行时间” 调整（如有必要）到与目前

升级相适应的值。这些值是为用户提供的信息。

8. 在各程序的“环境”选项卡，验证“程序可以运行”已设置为“无论用户是否登录”。

   这一设置会保证程序运行时有 Microsoft® Windows NT® Server 升级必需的管理权限。

9. 单击“确定”，关闭程序属性框。

10. 选择 Windows 2000 Server 程序包，从“操作”菜单上，单击“属性”。在“报告”选项卡上，为“版本”信息输入 *5.0*。验证“名称”为 Windows NT，“发行商”为 Microsoft。

    重要提示 要保证公布状态信息准确，必须设置这些值。否则，SMS 程序包执行的每一步都会被记录为成功，即便已经放弃或失败。

11. 单击“确定”，关闭程序属性对话框。

12. 如要确保在准备好部署 Windows 2000 前用户不能升级其计算机，请在新程序包下选择“访问帐户”，在结果窗格中，删除“来宾”和“用户”访问帐户。

    注意 SMS 会隐藏软件分发共享点，用户需要在计算机上有管理权限（或计算机运行 Microsoft Windows 95 或 Microsoft Windows 98 ）才能利用这些共享点。

    您需要为那些授权可在以后升级到 Windows 2000 的用户颁发访问权限。

同时，不要在这时调整分发点或创建公布。

警告 如想采取安全措施控制谁可以调整或部署程序包，请参见 *Systems Management Server 2.0 Administrator's Guide* 中的“Distributing Software”一章。

如果需要多个 Windows 2000 升级应答文件以适应升级的变化，必须在 SMS 管理员控制台中为程序包创建附加的程序。每个程序会为 winnt32 /unattend 开关指定不同的应答文件。 这些独立的应答文件让不同组的计算机只用一个程序包就可以按不同方式升级。

Systems Management Server 2.0 包括了程序包及其程序的各种复杂选项。例如，您可以指定 Windows 2000 文件可以在分发点以一个特定的共享名称得到。这样执行手动升级的人员和 SMS 就可以方便地使用这些文件。SMS 文档包括了这些选项的全部详细信息。

允许用户在升级时输入

大多 SMS 管理员认为不让用户在程序包安装时输入是一项好的做法。用户自己购买或安装软件时，安装程序通常会提示他们作出响应，例如把软件安装到哪个磁盘或安装哪些选项。每个用户交互都可能引入导致问题的错误。用户可能不理解所提供的答案的含义。即便只有小部分用户犯错误，在升级成千上万台计算机时，求助帮助中心的电话数量也会非常众多。

去除升级时用户输入的另一个原因是，可以允许进行无人参与计算机安装，以将安装带给用户的不便减至最小。

最后，在一个应答文件中提供所有应答也可以保证您能够维护配置标准。遵照这些标准，您可以减少可能导致问题的变量数目，从而简化以后的计算机维护和支持。

提供一个包含升级所需所有详细信息的应答文件，会避免 Windows 2000 安装程序要求用户输入。如果有些信息未提供（并且应答文件中的 UnattendMode 行允许），或没有指定 /unattend 命令行开关，程序会提示用户提供详细信息。服务器升级应答文件可能与以下类似（您需要更改 JoinDomain 行）。

```
[Unattended]
FileSystem = LeaveAlone
UnattendMode=FullUnattended
NTUpgrade=Yes
[Networking]
InstallDefaultComponents = Yes
[Identification]
JoinDomain = RED1DOM
```

备注 必须使用 winnt32 /unattend:answer.file 命令指定应答文件。winnt32 /unattend:answer.file 命令会执行无人参与升级，但它从当前配置获取所需的信息。

检查 Windows 2000 Server 程序包定义

Systems Management Server 2.0 附带的 Windows 2000 Server 程序包定义包括一些预定义程序。请查看这些程序,了解升级如何执行。

从 Windows NT Server 进行的 Windows 2000 Server 升级包括 /unattend30 和 /batch 开关。第一个开关，/unattend30 是指将进行无人参与升级，所有需要的信息从当前安装中获取。安装程序第一阶段完成，即将文件复制到计算机后 30 秒，计算机会重新启动。 它不使用应答文件。

/batch 开关指定安装程序不显示任何错误信息。这适合于将程序包发送给那些不想让安装程序牵涉的用户，或在无人看护计算机时运行升级。但如果升级出现问题，比如磁盘空间不足或“开始位置”目录错误，则这样做将不容易发现，因为没有错误消息显示。

但在作为运行结果生成的 SMS 状态消息中，需要包含错误信息。如果在测试中遇到问题而状态消息不够，请去除 /batch 开关，允许错误在程序包测试时显示。同样，如果用户在 Windows 2000 安装第一阶段单击“取消”按钮，则不会要求用户确认是否想要终止安装。

作为默认，程序包的“开始位置”目录被指定为 i386。这适合于程序包源包括一个映射 Windows 2000 CD-ROM 的 i386 目录的情况。但如果程序包源只包括 CD-ROM 上 i386 目录中及下级目录中的文件，则不需要指定“开始位置”目录。

SMS 2.0 程序包中的估计磁盘空间和运行时间是估计值，可能会与您的环境实际不符。您可能想要提高这些值。这些值仅是指示性的，是为了方便用户。

请注意“环境”选项卡，程序以 SMS 安全提供的管理权限运行。在将 Microsoft Windows NT Workstation 客户升级到 Windows 2000 Professional 时，这一点提供很大好处。这一功能意味着不需要将管理特权授予终端用户。在服务器为商业部门拥有，或中心管理员只能通过 SMS 拥有对服务器的权限时，它也尤为重要。

如果在程序包程序的命令行中加入一个应答文件，您就可以为升级指定多个选项。例如，可以指定 Windows 2000 安装到哪个磁盘，或是需要升级还是新安装。

准备 Windows 2000 Professional 升级程序包

要用 SMS 将用户计算机升级到运行 Windows 2000 Professional，必须先创建一个 Windows 2000 Professional 程序包。准备和使用这个程序包的方法与准备和使用 Windows 2000 Server 程序包非常类似。请按照创建 Windows 2000 Server 程序包的过程开始，但一定要指定是 Windows 2000 Professional 程序包。由于从 Windows95 和 Windows98 升级到 Windows2000 会有特殊的问题，您必须按下节所述的方式创建一个新程序。

备注 在使用 SMS 分发 Windows 2000 Advanced Server 时，还要确保创建一个单独的程序包。尽管这个程

序的许多文件和安装细节与 Windows 2000 Server 中相同，但它们还是有相当的差异，要求每个版本都有各自程序包。创建分发其它版本 Windows 2000 Server 的程序包时，您可以用基本 Windows 2000 Server 程序包定义作为起始点。

Windows 95 和 Windows 98 升级

除了源文件的差异，Windows 2000 Server 和 Windows 2000 Professional 升级的一个重要区别在于将 Windows 95 或 Windows 98 客户升级到 Windows 2000 Professional 时的应答文件中。运行 Windows 95 或 Windows 98 的计算机还不是域的成员（即使使用它们的用户登录到域），没有本地帐户（虽然它们拥有本地配置文件和密码列表文件）。因此在应答文件中必须说明相关的细节，如下例所示（必须更改 JoinDomain、DomainAdmin 和 DomainAdminPassword 的值）：

```
[Unattended]
FileSystem = LeaveAlone
UnattendMode=FullUnattended
Win9xUpgrade=Yes
[Networking]
InstallDefaultComponents = Yes
[GUIUnattended]
AdminPassword=Testing123
[Identification]
JoinDomain = RED1
DomainAdmin = AddComputers
DomainAdminPassword = Restricted
```

从 Windows 95 或 Windows 98 升级到 Windows 2000 的计算机被授予本地管理员帐户。该帐户需要密码；您可以在应答文件 GUIUnattended 部分指定密码，或在升级结束时提示用户输入。任何能够访问 SMS 数据包共享的人都可以从应答文件中读取该密码，通常是大多数的用户。这样做并不会有直接的安全风险，因为 Windows 95 和 Windows 98 计算机因为操作系统本身的非安全属性，在升级前并不具备安全性。

您可能想把管理员密码设置成安全的值，加强对管理特权的限制。这一点可以在升级之后，通过运行一个程序，把密码设置成只有授权人员共享的值做到。密码在程序内编译，未经授权的人员无法得到。使用通用编程语言或脚本工具如 SMS 安装服务很容易创建这样的程序。该程序可以用 SMS 分发，或在 Windows 2000 升级结束时通过在应答文件中指定适当的值对其调用。

运行 Windows 95 和 Windows 98 的计算机不是域成员，运行 Windows 2000 的计算机则必须是域成员。因此，需要在应答文件加入 JoinDomain 行，指出计算机加入哪个域，以及有权让计算机加入该域的管理帐户和密码。

警告 由于未经授权人员也可以读取应答文件，因此在创建时需要考虑安全问题。但人们一般不会从 SMS 分发点读取文件，因为分发点是隐藏的，而他们必须要知道到哪里去找这些详细信息。但可以采取适当的预防措施，即用一个只有“把工作站添加到域”权力的管理帐户。另一个预防措施是把以这种方式升级的计算机添加到专用的资源域。这样，管理帐户权利只需限于该域，从而不会导致可能有帐户域控制器等敏感计算机的其它域出现问题。

应答文件还应该指定想要升级的是 Windows 95 或 Windows 98 计算机。要做到这一点，请在应答文件加入下行内容：

```
Win9xUpgrade=Yes
```

如果没有这一行，则您做的是 Windows 2000 全新安装而不是升级。

从 Windows 95 或 Windows 98 升级到 Windows 2000 的过程中，Windows 2000 安装程序会删除认为可能与 Windows 2000 不兼容的程序。这种情况出现在一些 SMS 2.0 客户组件。Windows 2000 提供了一项称为迁移 DLL 的功能，简化了这类程序的迁移。有关迁移 DLL 的更多信息，请参见 Web 资源页的 Microsoft

Systems Management Server 链接，地址是：
http://windows.microsoft.com/windows2000/reskit/webresources。

Windows NT Workstation 升级

与从 Windows 95 或 Windows 98 升级相比，从 Windows NT Workstation 升级到 Windows 2000 要简单得多。这是因为 Windows NT Workstation 与 Windows 2000 Professional 有很多共同点。因此，不使用应答文件或者使用最小的应答文件就可以完成 Windows NT Workstation 的升级。

重要的一点是要设置 SMS 程序“环境”属性，这样它可以以带管理权的方式运行，不然，程序包在客户计算机端初始化时，用户需要登录并获得管理权。

分发 Windows 2000 程序包

您需要将 Windows 2000 SMS 程序包文件分发到打算升级的计算机所在的所有站点。即便只有一个站点，也要涉及到分发。分发包括以下步骤：将程序包文件发送到站点，然后把文件放到站点内的 SMS 分发点。

准备分发程序包

在分发 Windows 2000 程序包之前，还有几项任务必须完成，以确保 SMS 层次已做好接收准备。

检查站点服务器和分发点的状态

Windows 2000 是一个大型操作系统，需要相当大的磁盘空间。不仅要升级的计算机需要 Windows 2000 备份，SMS 在服务器间移动程序包时也需要备份。因此，必须查看站点服务器和分发点，保证它们有足够的磁盘空间。最简单的方法是，到 SMS 管理员控制台中的“系统状态”，选择“站点状态”，然后对每个站点分别单击“站点系统状态”，如图 14.4 所示。结果窗格会显示分发点及其可用的磁盘空间。

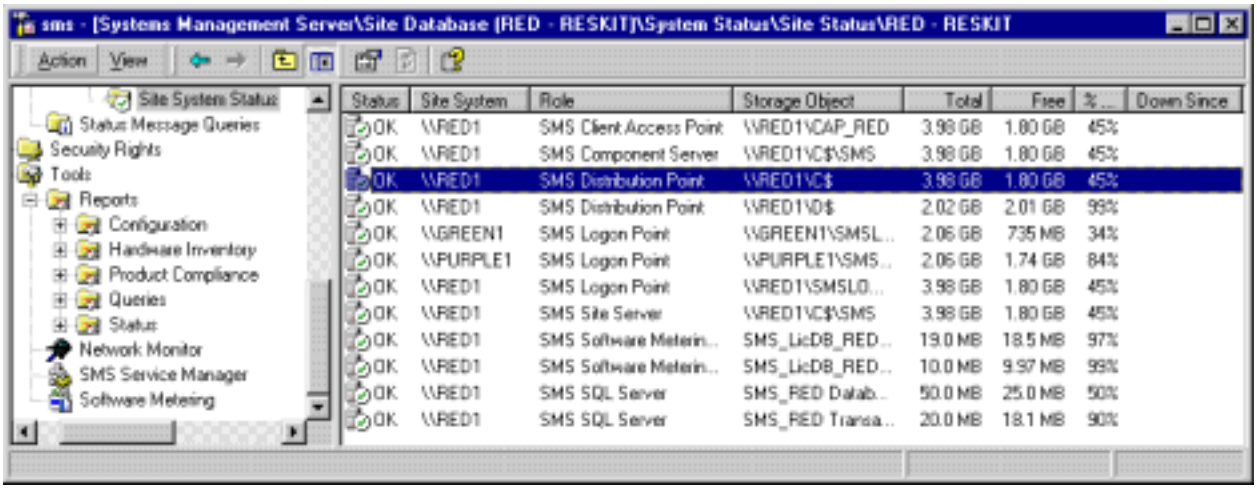


图 14.4 站点状态：分发点及其可用空间

确保每个站点有适当数量的分发点

有可能您想要限制在各个站点同时执行的 Windows 2000 升级数目。因为升级会给局域网络和分发点带来很

大负担。在升级之前，需要先在实验室中或运行先导测试程序进行试验。测试时，请使用能代表分发点的典型服务器和典型网络。这样就可以判断能够一次从容地升级多少客户。

如果发现升级的瓶颈不在网络而在分发点，请考虑给站点添加更多的分发点。有关如何添加分发点的更多信息，请看 *Systems Management Server Administrator's Guide* 中的“Distributing Software”。

使用分发点组

由于 Windows 2000 程序包很大并且需要广泛使用，因此要确认为它分配了分发点。您可以把这些分发点看作一个组。为 Windows 2000 分发点创建分发点组，可以减少管理任务的数量。

您可以在创建或调整分发点时，创建分发点组(以及给组添加或从组中删除分发点)。然后可以在分发过程中，在指定分发点的同一地点指定分发点组。

确保发送器控制就位

如果 Windows 2000 程序包发送到了任何没有合适发送器控制的站点，它就可能干扰其它的网络功能，导致网络链接过载。

因此，请检查发送器控制，确认它们已经正确设置。SMS 管理员控制台包括了各个站点的 SMS 地址定义。SMS 地址包括 SMS 站点服务器名称、访问站点的安全信息及网络传输详细信息（如果需要）。地址还包括一个指定了高、中、低优先级传输分别在何时执行以及一天中各个时间可以使用多少网络链接的日程安排。

确保输出端分发工作正常

Systems Management Server 2.0 有一项称为输出端分发的功能，允许子站点把软件分发到更低层的站点。这可以减少软件分发初始化站点的工作量，因为软件不需要再从初始化站点分发到所有站点，这也减少了初始化站点与其它站点之间网络链接的工作负荷，而这恰恰是最重要的问题。将程序包分发到许多站点、在网络间将 Windows 2000 频繁复制，都会造成不能承受的过重负荷。图 14.5 图示说明了有输出端和没有输出端软件分发的区别。

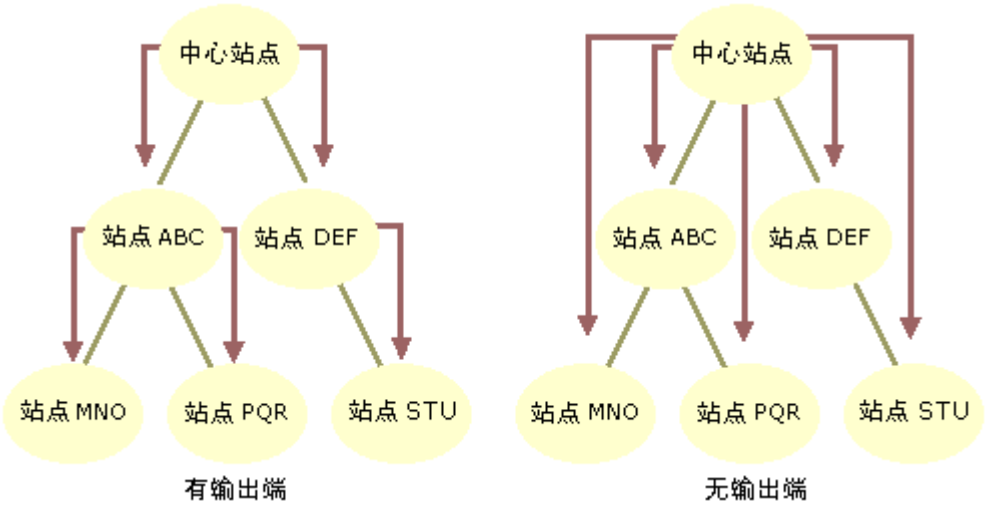


图 14.5 两种类型的软件分发

如果初始站点没有目标站点的 SMS 地址，则会自动进行输出端分发。因此，必须使用 SMS 管理员控制台查

看 SMS 地址，确保拥有站点地址的唯一 SMS 服务器是该站点的双亲。

选择测试站点

为确保您的规划已经完善，在将 Windows 2000 程序包分发到整个单位之前，请先将其分发到一个测试站点或少数几个站点。这样您就可以快速纠正问题，把问题的影响减至最小。

测试站点应尽可能典型，但也应该至少有一个站点代表了高风险方案。例如，使用只有很少多余磁盘空间的站点服务器或分发点的部署，或存在一个特别慢或不可靠的网络链接。

这一级测试的最佳做法是从没有复杂要求的小站点开始。理想的测试站点应该有技术专家随时提供支持，而且用户能够配合您的目标。在这些站点，您可以为任何部署过程中没有编入应急计划的问题找到相应的解决方法。随着对程序的信心增加，就可以把测试扩展到更大、更复杂或更难支持的站点。

在分发阶段，Windows 2000 部署应该对用户透明，因为还没有在他们的计算机运行升级。这时就应小心谨慎，在以后的部署过程这一点更为重要。

有关此处介绍的任务的更多信息，请参见 *Systems Management Server Administrator's Guide*。

将程序包分发到站点和分发点

分发程序包的基本程序如下所示。在执行这项任务时，请注意所有站点的所有分发点都已列出，这样您可以一次选择所有想要的分发点。但要确保先把程序包分发到少数几个站点，从而测试 SMS 基础结构和程序。随着信心的增加和容量的许可，您可以加入其它站点的分发点。有关这一流程的更多信息，请参见 *Systems Management Server Administrator's Guide* 中的“ 分发软件 ”。

要分发 Windows 2000 Server SMS 程序包，请

1. 在 SMS 管理员控制台中，选择“ 程序包 ”，选择 Windows 2000 程序包，然后选择“ 分发点 ”。
2. 从“ 操作 ”菜单，将鼠标指向“ 新建 ”，然后单击“ 分发点 ”。

   “ 新建分发点 ”向导出现。
3. 单击“ 下一步 ”越过欢迎页面，然后选择想用的分发点。

   如果是一个测试分发，请选择已确定的分发点。同样，如果在使用分发点组，请现在选定。注意所有站点的所有分发点都已列出，您可以选择所有想要的分发点。但为了更好地管理网络通信，您可以一次只做有限几个分发点。
4. 单击“ 完成 ”，启动分发。

警告 只要在第 4 步单击“ 完成 ”，分发过程就马上开始。您可能会注意到一个短暂的延迟，这是由于系统处理、程序包优先级或发送器时间安排等原因造成；但是请做好 SMS 活动马上开始的准备。

有关分发初始化后程序包流动的更多信息，请参见 *Microsoft® Systems Management Server 2.0 Resource Guide*（ *Microsoft® BackOffice® 4.5 Resource Kit* 的一部分）中的“ 软件分发流程图 ”。Windows 2000 文件被压缩成单个文件，然后发送到子站点。在各站点，如果有程序包的分发点，程序包就会随后发送到其它子站点。

测试分发

Windows 2000 程序包分发后，请验证它们已正常部署到各分发点。本章后面的“ 监视分发 ”一节，描述了

如何验证程序包已经到达所有分发点以及如何如何快速识别问题。但是，您还需要测试分发，确保分发完整并且目录树正常。这一级不需要测试所有的分发点，但一定要抽查一些分发点，以确认产品分发按意图进行。

扩展分发

第一次程序包分发成功完成后，您可以把程序包分发到其它站点和分发点。程序完全一样，除非您想以更少的监视、更高的频率、发送到更多的分发点。必须确保在程序包公布给站点的客户前将其分发到各站点。在分发点可用之前，SMS 使公布对客户不可用。

用 Courier Sender 分发

有些站点的网络链接可能速度很慢或不可靠，也可能已被其它通信完全占用。因此，在网络链接上发送象 Windows 2000 这样的大型程序包可能不能接受。SMS 2.0 包括了一个备用发送器，叫做 Courier Sender，它提供了所有 SMS 软件分发的好处，却无需通常的网络开销处理程序包发送到站点的工作。

使用 Courier Sender， SMS 程序包被复制到 CD-ROM 或类似媒体上，然后通过邮件或快寄发送到站点。在各站点，有人负责把 CD-ROM 放进站点服务器，并运行一个简单程序。软件分发从这点开始正常执行。公布、状态信息和其它信息会在指定的时间流过网络；但这一通信量比程序包本身需要的通信量要小得多。

监视分发

在一个有很多站点的单位内，分发 Windows 2000 很需要一些时间。由于广域网 (WAN) 链接速度、链接的可靠性、发送器时间安排等原因，有些站点需要的时间要比其它站点更多。还有可能尽管准备得很好，有些站点或分发点在程序包到达时没有充足的磁盘空间。基于上述原因，给 Windows 2000 分发预留适当的时间显得很重要。请认真监视，确定是否仍有问题需要解决，并确信所有站点的分发都已结束。

系统状态子系统

SMS 2.0 包含一个用来监视分发的强大的系统状态子系统。SMS 管理员控制台包括了“ 系统状态 ”节点，在这里您可以从系统状态子系统获取结果的摘要和详细数据。您也可以从“ 程序包状态 ”子节点得到程序包分发的状态。

备注 在创建程序包时，该程序包的定义会马上分发到所有子站点；但是，程序包的实际文件并没有分发。程序包定义更新后，相同的程序包定义会重新发送。然后就可以得到程序包定义分发状态信息。因此，在查看程序包状态时，要确认您已经分清了程序包定义分发和程序包文件分发。

软件分发状态可以归为如下几个层次：

所有程序包的程序包状态

当选中“ 系统状态 ”下的“ 程序包状态 ”时，您可以看到每个程序包有多少目标分发点，有多少已经安装、多少正在重试、多少已经失败，如图 14.6 所示。这一层次对识别有多少分发点（如果有的话）可能需要干预很有用。请注意原程序包和压缩程序包的大小不同。程序包标识号还可能有其它用途，如故障排除。

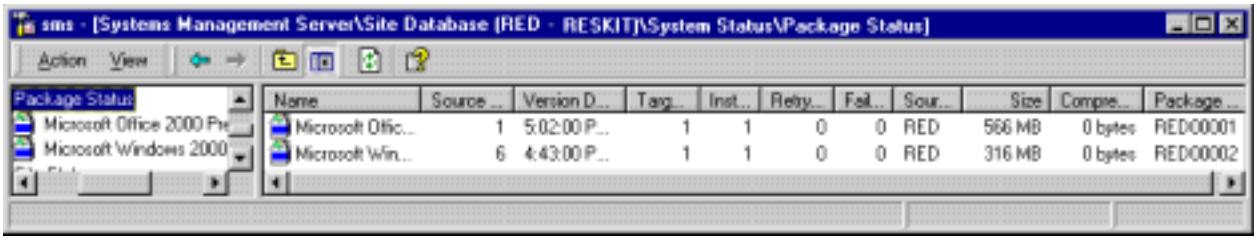


图 14.6 所有程序包的状态

在这一层次，没有状态消息可以查询。

特定程序包的程序包状态

在所有程序包的程序包状态下，可以选择各程序包。在这一层次您可以看到哪些站点应该而哪些不应该获得程序包，哪些站点需要干预，如图 14.7 所示。您还可以验证对所有站点，在“ 源版本 ”栏中都指出同一程序包版本。

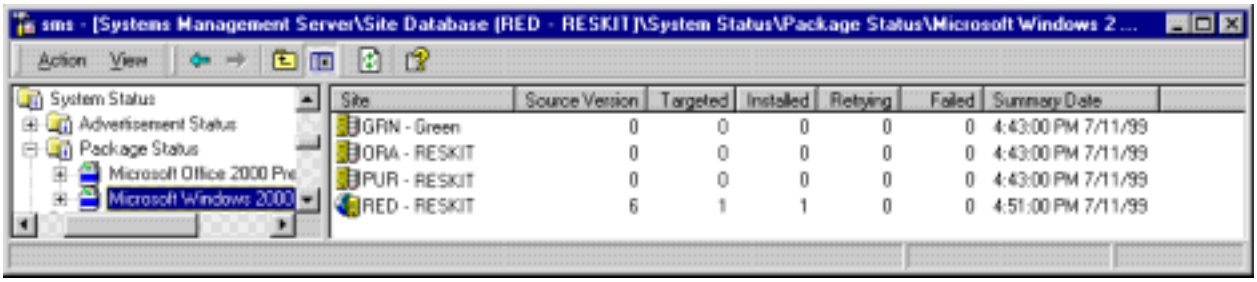


图 14.7 所有站点的 Windows 2000 程序包状态

在这个层次，可以选择“ 操作 ”菜单，然后选择“ 显示消息，全部 ”，查看所有站点和分发点程序包的全部状态消息。这可能有很多消息；因此最好单独查看每个站点的消息。

站点上的程序包状态

在特定程序包的程序包状态之下，您可以选择每个站点。这一层次的状态检查能让您看到，一个站点内哪些特定分发点可能有分发问题，如图 14.8 所示。

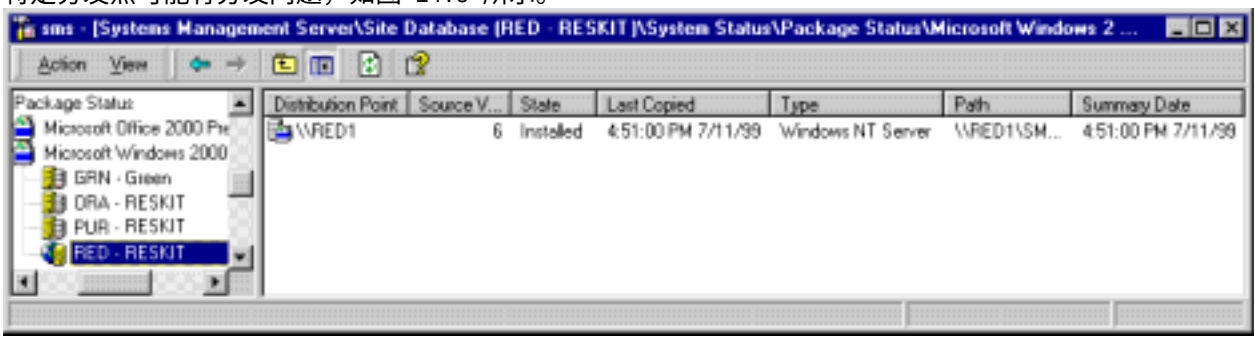


图 14.8 特定站点的 Windows 2000 程序包状态

这个层次，可以选择“ 操作 ”菜单，然后选择“ 显示消息，全部 ”，查看来自这个站点及其所有分发点程序包的全部状态消息。下面是典型的消息顺序（分发点特定消息在下节列出）：

- 30000 或 300001——程序包已创建或修改
- 30003——程序已创建
- 2300、2310 和 2311——分发管理器正准备程序包

- 2339——分发管理器正初始化日程安排和发送器，以发送程序包信息（不是程序包文件）
- 30009——分发点已指派
- 2333——正准备发送程序包压缩图像
- 2335——将程序包文件发送到站点的日程安排和发送器已由分发管理器初始化完毕
- 2315——程序包压缩图像已被分发管理器删除

在审阅状态消息时，请注意每个“ 分发管理器 ”活动序列都以消息 2301 结束，标志成功完成。只要“ 分发管理器 ”完成一项活动，该消息就会出现。“ 分发管理器 ”是 SMS 的组件，负责把程序包从站点服务器分发到 SMS 分发点，并初始化到其它站点的程序包发送。

分发点的程序包状态

在各个站点的程序包状态，您可以选择各个分发点。在这一层次，可以选择“ 操作 ”菜单，然后选择“ 显示消息，全部 ”，查看该分发点程序包的全部状态消息。下面是一个典型的消息顺序。

- 2317——分发管理器正刷新分发点的程序包（程序包第一次发送到分发点不会看到）
- 2342——分发管理器正开始把程序包分发到分发点
- 2322——分发管理器已将程序包解压缩到临时目录（如果适用）
- 2329——分发管理器已将程序包从临时目录或程序包源复制到分发点
- 2330——分发管理器成功地将程序包分发到分发点

备注 *Systems Management Server Resource Guide* 中有“ Status Messages ”一章，列出了所有状态消息和完整的消息文本。

报告程序包分发状态

可能您想生成一份程序包分发状态的报告，既可作为快速参考，也可满足您的特定需要。您可以执行程序包分发状态类别查询，并象在其它 SMS 报告工具所做的那样将响应并入选中 SMS 报告工具。表 14.1 列出状态信息的相关等级和类别，在每个状态信息中都能看到表 14.1 程序包分发状态类别

类别	状态信息
SMS_PackageStatus	分发点上程序包状态的总体摘要信息
SMS_PackageStatus RootSummarizer	给定程序包的信息。映射到 SMS 管理员控制台中“ 程序包状态 ”。
SMS_PackageStatus DetailsSummarizer	站点代码给定程序包的状态详细信息。映射到 SMS 管理员控制台“ 程序包状态 ”下的程序包控制台树。
SMS_PackageStatus DistPointsSummarizer	给定站点的给定程序包状态的详细信息。映射到 SMS 管理员控制台中“ 程序包状态 ”下程序包控制台树下的站点代码。

诊断分发中的故障

监视软件分发可以指明软件分发在一些点是否遇到问题。一般这是因为缺少磁盘空间、网络链接困难或服务器问题。状态消息文本指明了这类问题。

解决任何技术问题的第一步是把问题隔离开。知道了是哪个组件失败，您就可以把精力集中在相应问题上。使用前面介绍的监视技术，可以帮助您隔离问题。另外，*Systems Management Server Resource Guide* 中的“ Software Distribution Flowcharts ”一章中有些图形，显示了软件分发过程的典型流程。如果发现软件分发没有到达流程中的某个特定点，失败很有可能发生在流程图中的上一点。

隔离了特定组件后，通过了解工作原理就可以找到失败原因的线索。流程图对此也有帮助。另外，日志文件会显示底层组件的情况，继而发现哪些地方可能发生故障。 您可以使用 SMS Service Manager 启用日志文件。

Systems Management Server 2.0 Resource Guide 中的“ Software Distribution Flowcharts ”一章中也有软件分发故障排除的一些技巧。

公布 Windows 2000 程序包

用户在接收到公布后，就可以升级到 Windows 2000。公布会为终端用户提供程序包的描述信息，包括 SMS 运行程序必需的详细信息。公布甚至可以指派在特定时间运行，从而使用户不会妨碍升级，或在用户远离计算机时进行升级。

选择要升级的计算机

公布会告诉 SMS 程序包内的特定程序对 SMS 集合可用。集合是关于计算机、用户或用户组的非常灵活的定义。Windows 2000 软件分发时，您可以先使用少数计算机的集合进行测试。稍后，可以使用所有为 Windows 2000 做好准备的计算机集合。并可以把集合按站点或部门细分。

集合的另一个好处在于它是动态的；随着时间推移，您可以将计算机添加到集合，而对集合可用的公布会自动对添加的计算机可用。例如，如果集合基于计算机的内存容量，在为 Windows 2000 进行硬件升级后，计算机会添加到集合。如给计算机附加内存，SMS 硬件清单会检测到这一情况并记录在 SMS 中。则该计算机被自动加入集合；从而可以进行 Windows 2000 升级。与给计算机物理添加内存不同，这些都是自动完成的。

有关确定单位中哪些计算机已准备好升级的更多信息，请参见本书中的“ 使用 Systems Management Server 分析网络基础结构 ”。它包括定义查询，从 SMS 维护的清单中选择计算机。您可以如下列程序所述使用这些查询创建集合。SMS 还提供一个示例报告，Windows 2000 Upgrade Candidates by Site and Roles，可能对这一过程有所帮助。

要创建一个为 Windows 2000 做好准备的计算机的集合，请

1. 在 SMS 管理员控制台中，选择“ 集合 ”。
2. 从“ 操作 ”菜单，将鼠标指向“ 新建 ”，然后单击“ 集合 ”。
3. 在“ 集合属性 ” 对话框中输入集合名。
4. 在“ 成员身份规则 ”选项卡上，单击“ 新建查询规则 ” 按钮。
5. 在“ 查询规则属性 ”框中，单击“ 浏览 ”按钮，并选择适当的查询。

例如使用一个已经做好的查询，报告可以进行 Windows 2000 升级的计算机。（有关创建此类查询的帮助，请参见“使用 Systems Management Server 分析网络基础结构”一章。）您可能还想使用其它查询，例如“所有 Windows 95 系统”或已经包括特定站点所有计算机的查询。

6. 如有必要，添加查询规则和直接成员身份规则。

或者，您可以在第 4 步单击“新建直接规则”按钮，然后用“创建直接成员身份规则”向导指定想要升级的计算机。这在测试过程中可能是最佳选择，特别是在任意选择了几台计算机运行程序包时更是这样。

需要考虑的一个问题是 SMS 2.0 允许集合包含计算机、用户或用户组。在 Windows 2000 中包含用户或用户组可能并不合适，因为用户会经常登录到不同的计算机。因此，用户登录的每台计算机都可能被升级，特别是对于无论用户是否选中计算机，公布都会被指派并运行的情况。但用户登录的计算机可能并没做好升级准备，或是经常使用计算机的用户还没接受使用 Windows 2000 的培训。

警告 有关使用安全措施控制谁可以调整或使用公布的更多信息，请参见 *Systems Management Server Administrator's Guide* 中的“Distributing Software”。

准备要接收公布的客户机

要接收公布的计算机需要为公布做好准备。Windows 2000 升级过程中，计算机需要多次重新启动。如果可以自动进行，则整个升级过程不需要用户输入就能够完成。

有些用户在他们的计算机上设置了启动密码。密码是计算机本身要求的，因此软件无法绕过。不输入密码，计算机就无法重新启动，Windows 2000 升级就不能继续。因此，一定要告诉用户暂时取消启动密码。如果不能做到这一点，升级过程中必须有人在场。如果遇到硬件配置更改或其它问题，计算机在重新启动过程中停下来等待确认，也会出现同样的问题。

请将升级事先通知用户，让他们确认关闭所有文档。如果用户知道了即将升级，他们也会更愿意接受需要的任何培训、执行备份及准备好所负责的程序。

如果您公布的程序包指定通宵或周末运行，为了让公布自动开始,每台 Windows 95 或 Windows 98 客户计算机都需要有用户登录。这些用户可以用安全屏幕保护程序防止他人在他们不在的时候使用计算机。对 Windows NT 客户计算机，启动公布不需要用户登录。

将程序包公布到计算机上

现在您已经为分发准备好了程序包，选择了正确的计算机，并让计算机做好了升级准备。下一步就是初始化升级过程。请按以下程序创建一个公布，做到这一点。

要为 Windows 2000 创建公布，请

1. 在 SMS 管理员控制台中，选择“公布”。
2. 从“操作”菜单，将鼠标指向“新建”，然后单击“公布”。
3. 从“程序包”列表，选择 Microsoft Windows 2000 Server English。
4. 从“程序”列表，选择“从 NTS 3.51/4.0 (x86) 自动升级”。
5. 单击“浏览”，然后选择公布程序的目标集合。
6. 要设置公布在特定时间运行，请单击“日程安排”选项卡。要添加指派日程安排，请单击“新建”

按钮。

警告 指派的公布对每个公布客户只运行一次。如果公布在客户计算机处失败，客户不会试图再次自动运行。这可以保证计算机不会陷入运行指派的公布、失败、重新启动、然后重试的无休止循环中。因此，在第 6 步您可能还想选择“ 允许用户独立运行指派的程序 ”。这样，用户在程序首次运行失败时，可以比计划提前或滞后运行程序。或者，您可以在以后为升级失败的计算机新建一个公布。

与前面所述的 Windows 2000 软件分发阶段相同，请先在有限范围内启动公布，如果成功再将其扩展开来。这一点现在更为重要，因为终端用户肯定会受到软件分发的影响。要扩展公布，可以创建一些附加公布，每个附加公布以不同的集合为目标；也可以调整公布所基于的集合让它包含更多的计算机。把不同的程序公布到适当的集合可能需要不同的公布。例如，Windows 95 升级程序只能公布到 Windows 95 集合中的计算机。

扩展分发点上的安全

如果创建程序包时对分发点上的程序包访问做了限制，现在必须开放这些访问。请按以下程序开放这些访问。如果您正使用 SMS 运行有管理特权的程序，请把 SMS 站点使用的客户网络连接帐户添加为程序包访问帐户。

要开放 Windows 2000 程序包的安全设置，请

1. 在 SMS 管理员控制台中，选择“ 程序包 ”。
2. 选择 Windows 2000 程序包，然后选择“ 访问帐户 ”。
3. 从“ 操作 ”菜单，将鼠标指向“ 新建 ”，然后单击“ Windows NT 访问帐户 ”。
4. 在“ 访问帐户属性 ”对话框，单击“ 设置 ”。
5. 在“ Windows NT 帐户 ”对话框，输入域和用户或组，并指定“ 帐户类型 ”。单击“ 确定 ”，关闭对话框。
6. 在“ 访问帐户属性 ”对话框，验证“ 权限 ”为“ 读取 ”。

如有必要，重复该程序，添加其它用户或组。

升级计算机

如果在与要升级的计算机同一站点的分发点上已经有了 Windows 2000，并且公布在这些计算机上可用，就可以执行以下步骤：

- 把升级安排在用户方便的时间进行。
- 报告升级状态。

在每台计算机上执行公布

您可以在认为方便的时候，用 SMS 完成到所有用户的分发。但也可以让用户有调整日期和时间的权利，以在他们不用计算机时进行分发，如图 14.9 所示。您还可以在特定日期和时间强制升级，以免用户无限期地拖延。

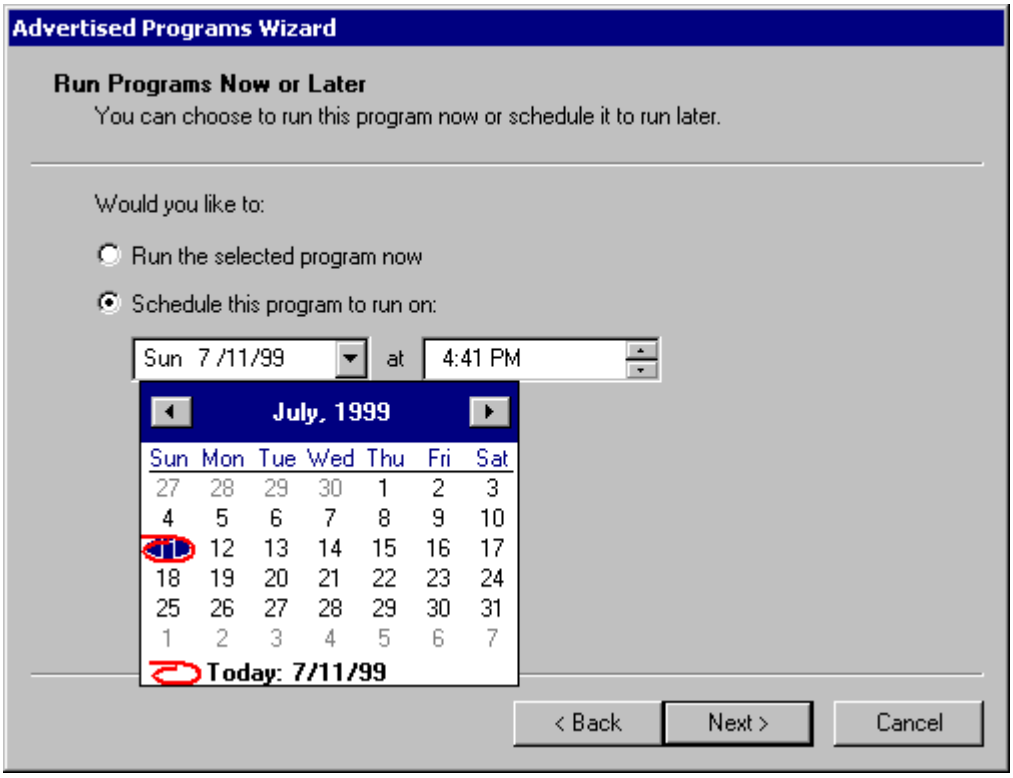


图 14.9 用户可以将升级安排在方便的时间进行

为用户启动的分发还要包括适当的命令行参数，指明使用哪个自动应答文件及其它选项，这样，安装可以按您确定的标准进行。

许多单位没有把客户计算机上的全部特权授给终端用户。这样做有助于将用户进行没有事先通知或无意的计算机改动导致的问题最小化。但没有特权会让用户无法为自己的计算机初始化 Windows 2000 升级。通过在特定的 SMS 安全帐户环境下进行 Windows 2000 升级，SMS 避免了这一问题。

各计算机的升级状态

Windows 2000 升级的最初和最后阶段完成时，Systems Management Server 会生成沿 SMS 层次结构向上传播的状态文件。这一信息可用来报告升级项目的整个进度，或用来调查单个计算机的状态，这一点将在下节进行讨论。

如果需要，可以生成自定义状态文件，指示升级状态相关的特定详细信息。创建这些状态文件的程序会作为程序包执行的一部分被调用，因此必须包含在定义中。例如，您可能想包含这样的状态文件，显示是否已让 Windows 2000 安装程序初始化升级后任务。

监视公布

报告每台计算机升级进度的 SMS 状态消息也可以用来报告 Windows 2000 整体部署进度。做好升级准备的计算机数、升级成功的的计算机数和失败的位置都可以进行报告。然后您可以对出现问题的地方做出干预。

系统状态子系统

SMS 2.0 包括一个强大的“ 系统状态 ”子系统，让您方便地监视分发。SMS 管理员控制台包含一个“ 系统状态 ”节点，在这里您可以从系统状态子系统获取结果的摘要和详细数据。另外还有一个“ 公布状态 ”子节点，可以让您获取公布的状态。

所有公布的状态

在 SMS 管理员控制台中选中“ 系统状态 ”下的“ 公布状态 ”时，可以查看以下内容：

- 有多少系统已经接收到公布。
- 多少系统在处理公布时经历了常规失败。
- 公布程序已经启动了多少次
- 程序运行完成或失败多少次
- 各种公布详细信息

图 14.10 中显示了该信息的一个范例。在这一层次，没有可查询的状态消息。

图 14.10 所有公布的状态

特定公布的状态

在所有公布的公布状态下，您可以选择每个公布。在这一层次，您可以查看以下内容：

- 哪些站点已有客户接收到公布
- 哪些站点有客户在处理公布时经历了常规失败
- 公布程序在每个站点运行了多少次
- 运行完成或失败了多少次

图 14.11 显示了这类状态。在这一层次，没有可查询的状态消息。

图 14.11 Windows 2000 公布的状态

站点的状态

在公布状态层次中，您可以选择每个站点。从“ 操作 ”菜单，将鼠标指向“ 显示消息 ”，然后单击“ 全部 ”，可以看到每个站点公布的状态消息。下面是一个典型的消息顺序。

- 30006——公布已创建
- 3900——公布已在站点内处理（分发到客户访问点，等等）
- 10002——客户接收到公布
- 10005——程序已启动
- 10007——程序失败

  该消息会说明失败发生的原因。通常原因是用户取消了程序或强制停止程序，或客户计算机磁盘空间不足。

- 10009——程序成功完成

  到这点，升级的 SMS 部分已经完成。这也是 Windows 2000 安装程序第一阶段（文件升级阶段）的结束。

- 13126——升级完成（如 SMS 2.0 SP2 或更新版本已到位，则报告成 10009 ）

  到这点，Windows 2000 安装程序完成。最后两个阶段（文本模式和 GUI 设置/安装）结束，计算机已准备好等待用户登录。

报告公布状态

为了方便参考或满足特定需求，您可能想生成一个公布状态的报告。您可以执行 SMS 公布状态子系统的查询，并象使用其它 SMS 报告功能一样把响应并入选中的报告工具。表 14.2 列出了状态信息相关的等级和类别

表 14.2 公布状态类别

类别	状态信息
SMS_AdvertisementStatusSummarizer	显示按站点代码分组的详细公布状态信息。映射到 SMS 管理员控制台中“ 公布状态 ”下的公布项。

有关基于 SMS 收集的数据撰写报告的更多信息，请参见 Web 资源页的 Microsoft Systems Management Server Technical Details 链接，地址是：
http://windows.microsoft.com/windows2000/reskit/webresources。

对于 Windows 2000 公布状态，您需要以下方式的报告：

已经做出公布但还没有接收到公布的计算机

这个报告与已在当前相关集合中但没有 10002 状态消息的计算机对应。如果程序已经在报告前公布，报告会指明最近没有使用或没有正确连接到网络或 SMS 基础结构的计算机。

已经接收到公布但还没有启动程序的计算机

这个报告与有 10002 状态消息但没有 10005 状态消息的计算机相对应。如果程序被指派在报告前运行，报告会指明自第一次公布以来没有使用或与网络或 SMS 基础结构连接断开的计算机。如果没有指派程序，报告还会包括用户选择不升级的计算机。

程序已启动但没有成功完成的计算机

这个报告与有 10005 状态消息但没有 10009 状态消息的计算机对应。这些计算机可能是因为用户取消了升级或计算机磁盘空间不足。解析 10007 消息描述可以得到更多详细信息。如果有任何问题是共有的，则有必要生成这些特定计算机的报告。

这里有一个细微的可能是，有些计算机失败，收不到 10007 或 10009 消息。

考虑到这种可能性，您可以报告有 10005 消息而没有 10008 或 10009 消息的计算机。

对于取消升级的用户，一封提醒他们升级重要性的电子邮件就可能足以解决问题。或者，可以指派一个程序在特定时间必须进行。对于其它问题，可能需要手动干预（使用 SMS 远程工具可能就够了）。

程序已成功完成但还没有接收到最终升级的计算机

这个报告与有 10009 状态消息但没有 13126 状态消息的计算机对应。这些计算机可能已经启动了升级但又由于某种原因终止。如果您在大量升级期间运行报告，比如在周末，这个报告就能帮助识别问题，并在用户知晓前将其手动纠正。但是，从生成 10009 消息到生成 13126 消息，升级通常需要处理一个小时以上时间。

备注 SMS 2.0 SP2 包括一个程序包状态报告系统的解决方法，13126 消息被代表正确行为的 10009 消息取代。这些消息的生成也更加可靠，同时 10009 消息带有一个有意义的消息文本，而 13126 消息没有文本。因此，建议您在使用 SMS 部署 Windows 2000 前部署 SMS 2.0 SP2。部署 SP2 后，报告逻辑就必须用消息文本辨别两个 10009 消息。

每天升级的计算机

这一报告是 13126 状态消息数按时间平分。这对监视项目整个的状态会有帮助。

诊断公布中的故障

公布监视过程可以帮助您在用户报告问题前隔离问题。典型的问题包括磁盘空间不足、用户干预或程序包定义错误。状态消息文本会显示这些问题。还要确保验证程序包至少在站点的一个分发点可用。

解决任何技术问题的第一步是把问题隔离开。如果知道是哪个组件失败，您就可以把精力集中在相应的问题上。使用前面列出的监视技术，可以帮助您隔离问题。*Systems Management Server Resource Guide* 中的“软件分发流程图”一章包含一些图片，显示了在服务器端软件分发的典型流程。同样在 *Systems Management Server Resource Guide* 中，“客户功能流程图”一章包含的图片显示了客户端的流程。如果发现软件分发没有到达流程中的某个特定点，失败很有可能发生在流程图中的上一点。

隔离组件后，理解工作的原理可以提供失败原因的线索。流程图对此也有帮助。另外，日志文件可以显示底层组件的情况，可以帮助您发现哪里可能发生故障。 您可以用 SMS 服务管理器启用服务器日志，而客户日志始终是启用的。

SMS 有几项功能可以帮助您解决客户计算机上的问题，包括：

- 远程控制客户计算机。
- 传送文件到计算机，替换需要升级的文件。
- 重新启动计算机。
- 通过日常事务清单或实时远程控制工具获取计算机详细信息。（注意即使客户脱机，日常事务清单也可用。）
- 升级不兼容应用程序软件。

可能会有需要手动干预的情况，比如升级导致计算机无法重新启动或无法与网络连接，或 SMS 客户组件不起作用时。

使用 Systems Management Server 简化域合并和域迁移

过去，较大的单位经常有多个域。使用 Windows 2000，保留这些域的原因似乎不再存在。因此，合并这些域可以简化计算机管理。而迁移到本机 Windows 2000 域可以让您的单位充分利用 Windows 2000 功能。

本书中的“确定域迁移策略”一章详细讨论了域合并和迁移的问题。该章还详细说明了可以简化合并和迁移过程的策略和技术。SMS 对这一过程也有帮助，因此使用 SMS 部署 Windows 2000 应该与域合并和迁移联系起来考虑。例如，您可以使用 SMS 为域控制器提交升级过程 DCPromo 部分的脚本可执行程序。

使用 SMS 进行域合并和迁移的最显著的好处是在 Windows 2000 的升级部署过程中。通过调整应答文件中的 JoinDomain 值，可以把计算机放入新建合并域中。

比较 Systems Management Server 1.2 与 Systems Management Server 2.0 之间的区别

Systems Management Server 2.0 与它的前版 Systems Management Server 1.2 明显不同。两个版本都有类似的功能设置，但各自实现其功能的技术却明显不同。如果计划使用 SMS 1.2 部署 Windows 2000 或进行域合并，您需要了解 SMS 1.2 软件分发在下列方面与 SMS 2.0 不同：

- 只有计算机可以作为软件分发的目标，且目标不是动态的（满足升级要求的新计算机必须作为新任务的目标）。
- 对于基于 Windows NT 计算机，登录用户不拥有管理特权，必须给出“程序包命令管理器”作为服务功能。SMS 1.2 的这个附加功不收费，但必须在开始 Windows 2000 部署前部署这个功能。
- 任务的状态子系统更难使用。
- 程序包原站点必须保留程序包的压缩备份。
- 程序不能强制另一程序在它之前运行，也不能集中停用。
- SMS 1.2 可能不支持 Windows 2000 计算机作为客户。因此在计算机升级到 Windows 2000 时，它们可能不再作为 SMS 1.2 客户运行，或不再被支持。有关 Windows 2000 计算机的 SMS 1.2 支持

的更多信息，请参见 Web 资源页的 Microsoft Systems Management Server 链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

两个版本的其它区别与可能有利于 Windows 2000 部署的其它 SMS 功能有关。有关这些功能和区别的更多信息，请参见本书中的“使用 Systems Management Server 分析网络基础结构”。

使用 Systems Management Server 部署 Windows 2000 的规划任务列表

表 14.3 列出了本章介绍的使用 SMS 部署 Windows 2000 的主要任务。

表 14.3 使用 SMS 部署 Windows 2000 的任务列表

任务	章节中的位置
学习 SMS 软件分发相关概念	使用 SMS 分发软件及比较 SMS 1.2 和 2.0 之间的区别
准备程序包	为 SMS 封装 Windows 2000
分发程序包	分发 Windows 2000 程序包
测试分发	分发 Windows 2000 程序包
监视分发	分发 Windows 2000 程序包
分发故障排除	分发 Windows 2000 程序包
报告分发	分发 Windows 2000 程序包
公布程序包	公布 Windows 2000 程序包
测试公布和程序包	公布 Windows 2000 程序包
升级计算机	公布 Windows 2000 程序包
监视公布	公布 Windows 2000 程序包
公布故障排除	公布 Windows 2000 程序包
报告公布	公布 Windows 2000 程序包
使用 SMS 简化域合并和迁移	使用 SMS 简化域合并和迁移

其它资源

- 有关使用 Systems Management Server 的更多信息，请参见 *Microsoft Systems Management Server Administrator's Guide*。
- 有关使用 Systems Management Server 的高级信息，请参见 *Microsoft BackOffice 4.5 Resource Kit* 中的 *Microsoft Systems Management Server 2.0 Resource Guide*。

第 15 章 - 升级和安装成员服务器

成员服务器提供文件、打印、Web、应用程序和通信服务。成员服务器不是域控制器，但每个成员服务器都在域中保留了帐户。可以将现有成员服务器升级至 Microsoft® Windows® 2000 Server 或安装新成员服务器作为 Windows 2000 Server 部署的第一阶段。这样在您部署 Active Directory™ 目录服务前就可以从 Windows 2000 Server 功能获益。本章所介绍的规划注意事项和步骤对系统管理员安装成员服务器或将其升级至 Windows 2000 Server 非常有用。

建议您对 Microsoft® Windows NT® 4.0 版、网络和联网概念和 Microsoft® Windows® 2000 站点有实际了解。这会对您确定在企业网络环境中 Windows 2000 Server 安装和升级的要求有所帮助。

本章内容

本章目标

本章将帮助您完成下列规划文档：

- 成员服务器安装和升级规划
- 现有硬件和软件清单

资源工具包中的相关信息

- 有关 Windows 2000 站点的详细信息，参见本书中的“设计 Active Directory 结构”。
- 有关制定测试规划的详细信息，参见本书中的“建立 Windows 2000 测试实验室”。

成员服务器升级和安装规划

安装或升级至 Windows 2000 Server 的一个主要好处是可以有 Active Directory™ 目录服务。但即使延迟安装 Active Directory，您也可以将成员服务器升级至 Windows 2000 Server。这样可以使用新的、经过改进的组件功能和服务，例如路由和远程访问、终端服务。

Windows 2000 域内的服务器可以充当下面两个角色之中的一个：作为域控制器或成员服务器。成员服务器是一个可以在 Microsoft® Windows® NT 3.51 版、Windows NT 4.0 或 Windows 2000 域中拥有帐户的 Microsoft 服务器。但如果是 Windows 2000 域的成员，它们就不包含任何 Active Directory 对象。成员服务器共享一般的安全功能，例如域策略和用户权限。

成员服务器可以作为：

- 文件服务器
- 打印服务器
- Web 服务器

- 代理服务器
- 路由和远程访问服务器

  应用程序服务器，包括：

  - 组件服务器
  - 终端服务器
  - 证书服务器
  - 数据库服务器
  - 电子邮件服务器

安装或升级至 Windows 2000 的过程

成员服务器安装或升级规划过程要花费相当的时间。事先规划可以使网络升级出现的问题减少到最低程度。图 15.1 是设计适合网络基础结构的升级策略的推荐步骤。

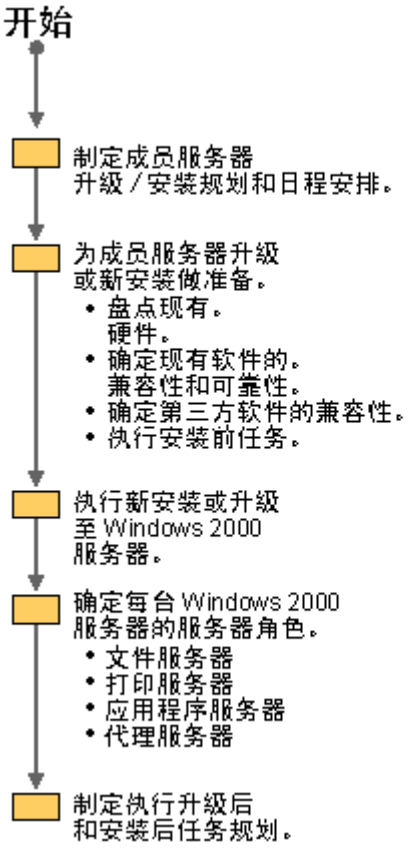


图 15.1 成员服务器安装和升级步骤

制定升级和安装规划

完整的规划有助于部署顺利运行。除了前面的流程图，下面的指导方针也可以帮助您制定成员服务器升级和安装规划：

- 如有必要，修改任何现有网络设计文档，反映您当前服务器环境。

  如果没有最新网络布局图，考虑在进行网络升级前绘制一个。

  从下列方面检查现有网络基础结构：

  - 软件兼容性
  - 互操作性需求
  - 硬件需求

  解决下列问题：

  - 需要多少新成员服务器？
  - 哪些成员服务器应该升级？
  - 哪些成员服务器应该在升级前替换成新硬件？
- 记录当前网络环境中的变动并明确相关规划的注意事项。
- 如有需要，建立测试环境，这样部署前可以测试可能有不兼容软件的成员服务器。

制定日程安排

升级服务器时，通常会出现网络服务中断。为将这种风险降低到最低程度，确立升级最后时限，减少运行时间内的停机时间。在确立时限和升级日程安排时，要考虑以下方面：

单一服务器安装或升级允许的时间量 升级服务器需要的时间量取决于硬件速度和安装操作系统后安装的应用程序和服务的数量和种类。有经验的管理员可以在大约一小时内在单一服务器上安装或升级操作系统。但在服务器真正投入网络运行前的安装评估和测试可能会花费几小时甚至数天。

实现 Windows 2000 Server 的新服务和功能 安装或升级服务器后，可以给它配置新服务或功能。这包括在将服务器安装到运行网络前，先在测试实验室环境中对其进行测试。

方案：尽量缩短服务器升级时网络停机时间

尽量缩短停机时间的最佳方案之一是分阶段安装或升级成员服务器。例如，一个总共有 70 台服务器的网络运行 Microsoft® Windows® NT Server 4.0 版，并且有不同类型的成员服务器。除了现有的成员服务器，管理员参考网络增长分析，决定还需要 5 台服务器才能满足下一年度的网络增长要求。为使其它服务器和客户机仍能访问 Internet、文件和应用程序，管理员不能一次升级所有服务器。这个示例网络中的每个成员服务器组的类型和数量如下：

- 5 台文件服务器（将添加 1 台新的文件服务器）
- 10 台应用程序服务器（将添加 1 台新的应用程序服务器）

- 10 台 IIS 服务器
- 5 台传真服务器
- 5 台代理服务器
- 10 个路由器（将添加 1 个新的路由器）
- 5 台路由和远程访问服务器（将添加 1 个新的路由和远程访问服务器）
- 15 台打印服务器（将添加 1 个新的打印服务器）
- 5 台 SQL 数据库服务器

首先，管理员确定升级每组成员服务器需要多长时间。管理员决定将一种类型的服务器脱机，在正常办公时间内升级并测试，其余服务器联机工作。如果升级和测试进展顺利，其余服务器将在正常办公时间过后的夜晚升级，让已升级服务器处理网络业务。添加的服务器的安装将在所有原有服务器升级后进行。这样可以有时间配置新服务器的服务和组件。

为成员服务器升级或新安装做准备

安装或将成员服务器升级至 Windows 2000 Server 要求计算机与新的操作系统兼容。为成员服务器成功升级或安装做准备，您需要执行不同的任务，收集不同信息。

盘点现有硬件

准备成员服务器首先要盘点现有硬件。要做到这一点，记录每个成员服务器的下列信息。

- 每台要升级计算机的供应商、型号和型号。
- 已安装的物理内存量。
- 已安装的网络适配器类型。
- 所有即插即用设备。
- 与服务器连接的不间断电源 (UPS)。
- 与计算机连接的外置硬盘类型。
- 硬盘分区和可用的空闲磁盘空间。
- 正在使用的任何硬件或软件独立磁盘冗余阵列 (RAID)。
- 已安装的 CD-ROM 驱动器类型。

确定系统要求

Windows 2000 Server 的系统要求比 Windows NT Server 4.0 更高。为保证 Windows 2000 Server 有效运行，网络上的每台服务器必须满足最低要求。最低硬件要求如下：

- 166-MHz Pentium 或更快的处理器。

Windows 2000 Server 的新安装程序最多支持有 4 个处理器的计算机。如果您升级的计算机运行支持多于 4 个处理器的 Windows NT Server，您必须升级至最多支持 8 个处理器的 Windows 2000 Advanced Server。

- 至少要有 64 MB RAM，推荐值是 128 MB，最大值是 4 GB。
- 硬盘分区要有与安装过程相适应的足够的可用空间。

  在计算需要的空间时，起点是 850 MB 加计算机内存量的两倍值。是否还需要更多空间取决于下列因素：

  - 安装的组件和服务。
  - 使用的文件系统。

    文件分配表 (FAT) 文件系统需要 100 至 200 MB 的额外空闲磁盘空间。

  - 安装使用的方法。

    要在网络安装，必须允许 100 至 200 MB 的额外空间，与从操作系统 CD 安装相比，这一过程中附加驱动程序文件必须可用。

  而且，升级需要的磁盘空间可能比全新安装多得多。由于添加了 Active Directory，现有用户帐户数据库可以最大扩大 10 倍。

备注 完成安装后，操作系统实际使用的磁盘空间（用户帐户除外）通常比安装程序要求的可用空间小，这取决于安装哪个计算机组件。

有关其它要求的信息，参见 Windows 2000 Server 操作系统 CD 上的 \Support 目录。

确定现有软件的兼容性和可靠性

非常重要的一点是在升级前确保您需要使用的软件与 Windows 2000 兼容。通过与软件供应商联系或建立运行应用程序的测试网络，可以做到这一点。

另外，为帮助确定现有软件是否兼容和可靠，您还要解决下列问题：

- 正在使用的是哪个文件系统 (FAT 还是 NTFS)？
- 当前使用的是哪个操作系统和服务包 (Service pack)？
- 程序针对哪个操作系统编写（Microsoft® Windows NT®、Microsoft® Windows® 98、Microsoft® Windows® 95、Microsoft® Windows® 3.*x* 还是 Microsoft® MS-DOS®?）
- 程序是针对特定网络环境编写的吗？针对的是网络的哪个版本？
- 程序和程序配置文件存储在服务器上还是客户机上？
- 数据文件存储在服务器上还是客户机上？

回答完这些问题，您就知道您的环境中的现有软件是否与 Windows 2000 Server 兼容。

确定第三方软件的兼容性

Windows 2000 Server 软件是符合徽标的软件（为 Windows 2000 Server 设计的软件），它采用了 Windows 2000 Server 功能，如 Active Directory。为 Windows 2000、Windows NT、Windows 95 或 Windows 98 编写的软件都应在 Windows 2000 Server 下正常运行。为 16 位 Windows (Windows 3.*x*) 或 MS-DOS 编写的软件应该可以在 Windows 2000 Server 环境中工作，但要考虑以下几点：

- 软件可能需要特定配置文件，如 Autoexec.nt 和 Config.nt。
- 16 位软件可能有或需要已不可用或与 Windows 2000 Server 不兼容的特定设备驱动程序。在这种情况下，与编写软件的供应商联系，看他们是否有或正在开发您需要的设备驱动程序。

在任何情况下，应该在实验室环境下 Windows 2000 平台上彻底测试所有软件，以避免在生产环境中存在的停机和数据损失风险。有关建立测试环境的详细信息，参见本书中的“ 建立 Windows 2000 测试实验室 ”、“ 实施 Windows 2000 先导测试 ”和“ 测试应用程序与 Windows 2000 的兼容性 ”。

执行安装前的任务

建议您执行特定任务以确保系统文件安全和安装顺利进行。这些任务包括：

阅读安装前文档

有三个重要文档网络管理员应该在执行升级前阅读：

- 硬件兼容列表

  硬件兼容列表 (HCL) 包含帮助您确定当前硬件是否与 Windows 2000 Server 兼容的硬件兼容信息。这个列表很全面，但请注意 Microsoft 在不断地更新信息。要确定您单位的硬件是否在 HCL 中，参见 Web 资源页的 Hardware Compatibility List 链接，网址是:http://windows.microsoft.com/windows2000/reskit/webresources。

- Read1st.txt

  Read1st.txt 文件提供最新的、关键的或其它安装前和升级信息，它是 Windows 2000 Server 文档的补充。

- Relnotes.txt

  这个文档提供最新的、或有关 Windows 2000 Server 的发行说明，同时也是文档的补充。此文件包含对操作系统附加组件的详细技术说明。可以用它作出有关网络中成员服务器部署的决定。

记录系统信息

升级开始前记录每台服务器的所有相关系统信息很重要。如果有必要将成员服务器复原到初始状态，这些记录可以提供一个重要的参考文档。

要查看 Windows NT Server 4.0 中的服务器系统信息，从“ 管理工具 ”菜单，单击“ Windows NT Server 诊断 ”。要打印该信息，从 Windows NT Server 诊断管理器单击“ 文件 ”和“ 打印报告 ”。

进行升级或安装

决定在成员服务器上执行 Windows 2000 Server 升级还是全新安装取决于当前服务器是否已经有 Windows NT 操作系统或是否准备将新服务器布置到基础结构中。

升级前任务表

启动 Windows 2000 Server 安装向导前，检查下列任务表，应用可能适用于网络基础结构的成员服务器的任何任务。

检查事件日志看是否有错误。

在 Windows NT 4.0 下的“事件查看器”中检查系统、应用程序和安全事件日志，确保当前没有任何错误记录。如果发现错误，在升级至 Windows 2000 Server 前改正。

备份系统文件和重要文件。

执行计算机上所有驱动器的完全备份。升级前保存重要的硬盘安装程序信息。

在 Windows NT 4.0 中，可以使用“磁盘管理器 (windisk.exe)”将硬盘分区表存到软盘上。在菜单栏单击“分区”，然后单击“配置”和“保存”。

如果驱动器是用 NTFS 文件系统格式化的，就不需要采取任何步骤准备磁盘。Windows 2000 Server 安装程序会将它们转化成 Windows 2000 Server 中使用的 NTFS 版本。同时禁用磁盘镜像，因为镜像卷在另一个驱动器上保留一套复制的数据，减少了发生不可恢复错误的可能性。如果升级时启用镜像，而且主驱动器上的数据损坏，可能导致镜像驱动器上的所有数据丢失。

还有，将所有重要文件备份到磁带或网络的一部分上。如果升级出现问题，为了保护您的数据，先完成这一步非常重要。

如果您使用备份功能，检查位于 \Winnt\Backup.Log 的备份日志，确认备份过程完成后没有出现错误。

您也可以使用 Microsoft® Windows NT® Server Resource Kit 所带 CD 上的 Regback.exe 程序备份成员服务器注册表。这个工具无需使用磁带就可以备份文件的注册表项。但是，Windows 2000 Server 会在备份系统状态数据时一起备份注册表。

删除不兼容软件和实用程序。

删除任何病毒扫描程序、第三方网络服务或客户软件。有关具体应用程序问题的信息，参见发行说明文件（在 Windows 2000 Server 操作系统 CD 上）。

断开 UPS 设备。

断开与任何 UPS 设备连接的串联电缆。Windows 2000 Server 试图自动检测连接到串行端口的设备，这些设备可能导致 UPS 和安装过程出问题。

如有可能，设置系统 BIOS 以使其保留非即插即用 ISA 设备当前使用的所有中断请求 (IRQ)。不做到这一点可能导致安装过程中出现下列提示信息：

INACCESSESSIBLE_BOOT_DEVICE

如果是这样，您就无法完成安装。

还要确保更新紧急修复磁盘和紧急启动磁盘。

升级成员服务器

升级成员服务器有一个基本上自动完成的流程。升级期间，Windows 2000 Server 迁移操作系统当前设置，很少需要管理员输入。

升级计算机时，先放入 Windows 2000 Server 操作系统 CD，然后安装向导会指导您按步骤升级。看到提示后，单击“升级至 Windows 2000”。最后一步完成后，Windows 2000 Server 安装程序重新启动，收集信息，使用上一个操作系统的已有设置。

执行新安装

在没有操作系统的计算机上安装 Windows 2000 Server 有三种方法：

- 如果计算机支持 CD-ROM 驱动器作启动设备，插入操作系统 CD 后安装程序自动启动。确保系统 BIOS 配置允许 CD 自动启动。

  备注 在许多计算机上自动启动功能默认时不启用，但可以手动启用该功能。

- 如果计算机不支持 CD-ROM 驱动器作启动设备，您需要使用四张安装盘安装 Windows 2000 Server。
- 如果您选择从网络安装操作系统，您需要能够识别当前计算机上安装的网络适配器的网络客户磁盘。这样您就可以登录到相应的域。

  备注 如果您从网络安装 Windows 2000 Server，您的客户端许可证数量要满足安装的服务器数量要求。

对于新成员服务器，初始安装时没有已存在的服务或应用程序。这样，您的计算机会兼容 Windows 2000 Server，并且满足本章前面说明的所有系统要求。计算机需要在局域网 (LAN) 上或有一个受支持的 CD-ROM 驱动器，并有格式化的硬盘。

确定每台 Windows 2000 Server 的服务器角色

成员服务器在网络上可以有不同的功能，管理员可部署不同的服务，在网络基础结构中形成中间层。下面几节讲述每个可能的角色，并在必要时提供每种服务器的安装和升级的详细信息。

文件服务器

文件服务器给部门和工作组提供访问文件的权限。在以前的各 Windows 服务器操作系统中，文件共享只限于在站点内 — 如果用户要访问他们需要的文件，必须与一个一个的文件服务器连接。如果一个文件服务器不能访问，用户就要访问包含相同文件的其它文件服务器。有了 Windows 2000 Server，就没有必要访问共享了。

使用 Windows 2000 Server 分布式文件系统 (Dfs) 可以跨站点或跨域分布 Windows 2000 Server 文件服务器上的共享文件。有了 Dfs 基础结构，一组文件服务器可以看成一个整体。例如，请看下列 Windows NT 4.0 文件服务器名称：

- \\fileserver\file1
- \\fileserver\file2
- \\fileserver\file3
- \\fileserver\file4

用 Windows 2000 Server Dfs，可以将这四个文件服务器全部添加到 Dfs 树中，而只使用名为 \\fileserver 的一个共享。这样任何客户都可访问这四个文件服务器中的任何一台服务器上的任何文件。这就实现了冗余和负载平衡，因为 Active Directory 首先尝试联系离请求信息的客户最近的文件服务器。如果该文件服务器不可访问，Dfs 就到下一个文件服务器去获取信息。

如果计划用 Dfs 跨域分布文件服务器，建议您在升级前规划好哪些服务器分发哪些文件共享。例如，将所有的存储应用程序的文件服务器全部放入名为 \\Fileserver\Applications 的组中。下一组存储备份数据的文件服务器组可以命名为 \\Fileserver\Backup 。这样可确保用户在确定需要使用哪个文件共享时不易混淆。

有关规划安装、配置和使用 Dfs 的详细信息，参见《Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide》中的“ 分布式文件系统 ”和本书中的“ 确定 Windows 2000 存储管理策略 ”。

备注 基于域的 Dfs 要求 Active Directory 必须运行。

Macintosh 卷

升级带有 Macintosh 卷的 Windows NT 4.0 文件服务器时，要确保用于 Macintosh 的服务已经升级（如果升级前将其删除，则要重新安装）。还应确保升级之前备份 Macintosh 文件。那么您就可以按照本章前面的操作指南将服务器升级至 Windows 2000 Server。

升级完成后，可以使用“ 计算机管理 ”功能查看迁移后的 Macintosh 卷，如图 15.2 所示。

图 15.2 显示迁移后的 Macintosh 文件卷的计算机管理

在 Windows 2000 Server 中可以采用 AppleTalk 或 TCP/IP 协议访问 Macintosh 卷。如果网络上有的客户只使用 AppleTalk，则可以通过“ 控制面板 ”内的局域属性安装协议。

如果您要安装新文件服务器作为 Macintosh 卷主机，第一步要验证硬件是否满足最低要求。参见本章前面给出的任务列表和 Windows 2000 Server 操作系统 CD 上的 HCL。然后按照本章前面给出的操作指南安装 Windows 2000 Server。

安装完成后，使用“配置服务器”向导并单击“文件服务器”，或到“管理工具”下的“计算机管理”单击“共享文件夹”，这样新服务器便成为 Windows 2000 文件服务器了。

Novell NetWare 卷

用于 NetWare 的 Microsoft 文件和打印服务是一个实用程序附件，它们能使运行 Windows 2000 Server 的计算机能够直接向 NetWare 和其兼容客户机提供文件和打印服务。对 NetWare 客户机而言，服务器与其它任何 NetWare 服务器一样，客户可以访问服务器的卷、文件和打印机。对 NetWare 客户软件不需要进行任何更改或添加任何附件。

这个实用程序是 Microsoft 产品 (Microsoft Services for NetWare v. 5: Add-on Utilities for Microsoft Windows 2000 Server and Microsoft Windows NT Server 4.0) 的一个组件。

测试文件共享

成员服务器升级至 Windows 2000 Server 后，应确保您仍可以按下面这些步骤访问共享。

- 从服务器打开 Windows 资源管理器。单击两个或三个文件共享，在“文件”菜单上，单击“属性”，然后选中共享复选框。
- 从一台或多台客户机登录并映射几个已知共享的驱动器，验证在 Windows 2000 Server 上共享工作是否正常。

如果升级服务器以支持 Dfs，应确保在交替关闭每个文件服务器并执行同样步骤时，能访问到所有文件服务器。

打印服务器

单位无论大小都要求具有用户能在几个站点和域之间使用打印功能的能力。单位的大部分打印都在组内设置，以方便组内所有用户访问。打印机可以设置成公用打印机，以便在全局范围内都能使用；或设置成专用打印机，以便只有组内的一部分或特定用户才可以访问。这需要仔细规划有权访问特定打印机组的用户数量。

打印服务器安装

安装 Windows 2000 Server 打印服务器的要求如下：

- 服务器运行 Windows 2000 Server。
- 服务器有足够的 RAM 处理文档。

  如果打印服务器管理很多打印机，服务器需要的 RAM 比 Windows 2000 Server 所要求的 RAM 更大，这样才能处理其它任务。如果打印服务器的 RAM 不足以处理它的工作负荷，打印性能就会下降。

- 服务器有足够的磁盘空间以在打印前后台处理文档。

  这一点在文档很大或有很多文档等待处理时很重要。例如，如果 10 个用户要同时打印，在打印服务器将文档发送到打印设备之前，打印服务器必须有足够的磁盘空间保留所有文档。若服务器内存不足，文档一直停留在客户机上，直到服务器有足够的空间，这样会导致客户机的性能下降。

- 安装所有正确的打印驱动程序。

  正确的打印机驱动程序是指那些为 Windows 2000 Server 编写的程序。可以在 Windows 2000 Server 操作系统 CD 上找到正确的驱动程序或从打印机制造商那里获取。用于不同硬件平台的打印机驱动程序不可通用。

不运行 Microsoft 操作系统的客户机要想打印到网络打印机还有其它要求。必须在打印服务器上安装其它服务并在客户机上安装正确的打印驱动程序。这些服务包括：

- Macintosh — 为 Macintosh 提供的服务
- NetWare — 用于 NetWare 的客户机和网关服务。
- UNIX TCP/IP 打印 — 也称为行式打印机守护程序 (LPD) 服务。

与打印机制造商联系，索取正确的驱动程序。

安装网络打印环境的指导方针

如果您现在还没有网络打印环境，则要按照下列指导方针制定网络范围的打印策略。

- 确定需要打印的用户的数量及他们可能产生的打印工作负荷。
- 确定打印要求。例如，如果销售部门的用户需要打印彩色的小册子，就需要安装彩色打印设备。
- 确定打印机的位置。打印机应放在用户取打印文档时非常方便的地方。
- 确定打印服务器数量以便满足网络上的打印机数量和类型的需要。

  应考虑以下几个方面：

  - 共享打印机应允许多个用户打印到一台设备。
  - 打印机池应允许多个打印机共享打印队列。打印设备应该是相同的且位置接近，除非它们共享公用仿真模式。
  - 打印机优先权应允许打印队列按分配给用户或用户组的优先权处理某些打印作业（与按时间顺序处理不同）。

Active Directory 与 Windows 2000 Server 打印服务集成

可以通过实现 Active Directory 来增强网络打印能力。但值得注意并且很重要的一点是即使不部署 Active Directory，Windows 2000 Server 打印服务的性能和功能也能够增强。

部署 Active Directory 后，Windows 2000 服务器提供一个标准的打印机对象。有了这个对象，可以发布打印机让其能够在 Active Directory 中跨网络共享。这给用户提供了一个简单的在 Active Directory 结构中搜索打印机的方法。用户能够查找打印机属性，如打印功能（PostScript，色彩，纸张大小等）和打印机位置，包含与其连接和发送文档的性能（取决于打印机权限）。

测试打印机共享

安装 Windows 2000 Server 或将打印服务器升级至 Windows 2000 Server 后，按照下列步骤执行测试以确保所有打印机共享都能正常运行。

要测试打印服务器安装

1. 在“ 控制面板 ”，打开“ 打印机 ”文件夹。
2. 在“ 文件 ”菜单上，单击“ 属性 ”。打印机“ 属性 ”窗口出现。
3. 在“ 属性 ”窗口，单击“ 打印测试页 ”。
4. 确认所有打印机共享在 Windows 2000 Server 下正常运行。

在服务器上给每台打印机打印测试页后，从多台客户机重复测试，验证它们能否映射到打印机共享并提交打印作业。

应用程序服务器

应用程序服务器可为多个用户使用的程序提供集中的位置。可以让用户通过一个共享访问应用程序，而不用将应用程序安装到 1,000 台客户机上。这样的服务器可能需要配置很高的资源，这取决于使用程序时需要的磁盘存取量。例如，用于数据库程序的应用程序服务器可能比字处理程序服务器需要更多的内存和磁盘空间。

执行新的 Windows 2000 Server 安装或从 Windows NT 4.0 升级时，应确保备份与用于 Windows 2000 Server 的应用程序相关的数据。在备份应用程序和数据后，在测试环境升级应用程序服务器以确保兼容。

应用程序成员服务器可作为多种程序和服务的主机。参见表 15.1 是对部分服务的说明。

表 15.1 应用程序成员服务器上的程序和服务

服务	说明
组件服务	管理服务器组件，如应用程序负载平衡、事务服务、应用程序管理和消息队列。
终端服务	允许客户应用程序在服务器上运行的软件服务，这样客户机作为终端而不是独立系统运行。
数据库	为数据库程序（如 Microsoft® SQL Server™）提供操作和管理平台。
电子邮件	为邮件服务器（如 Microsoft® Exchange Server） 提供操作和管理平台。

备注 对数据库和邮件服务器，其它应用程序需要安装在 Windows2000 上。Windows2000 本身不具备这些服务。

安装 Windows 2000 Server 后可以用“ 配置服务器 ”向导配置这些服务，但 Microsoft® Exchange Server 和 Microsoft® SQL Server™ 除外。

组件服务

应用程序成员服务器为运行诸如应用程序负载平衡、事务服务、应用程序管理和消息队列之类的组件服务提供平台。可以通过“ 添加/删除程序 ”和“ Windows 组件向导 ”添加这些服务，如图 15.3 所示。

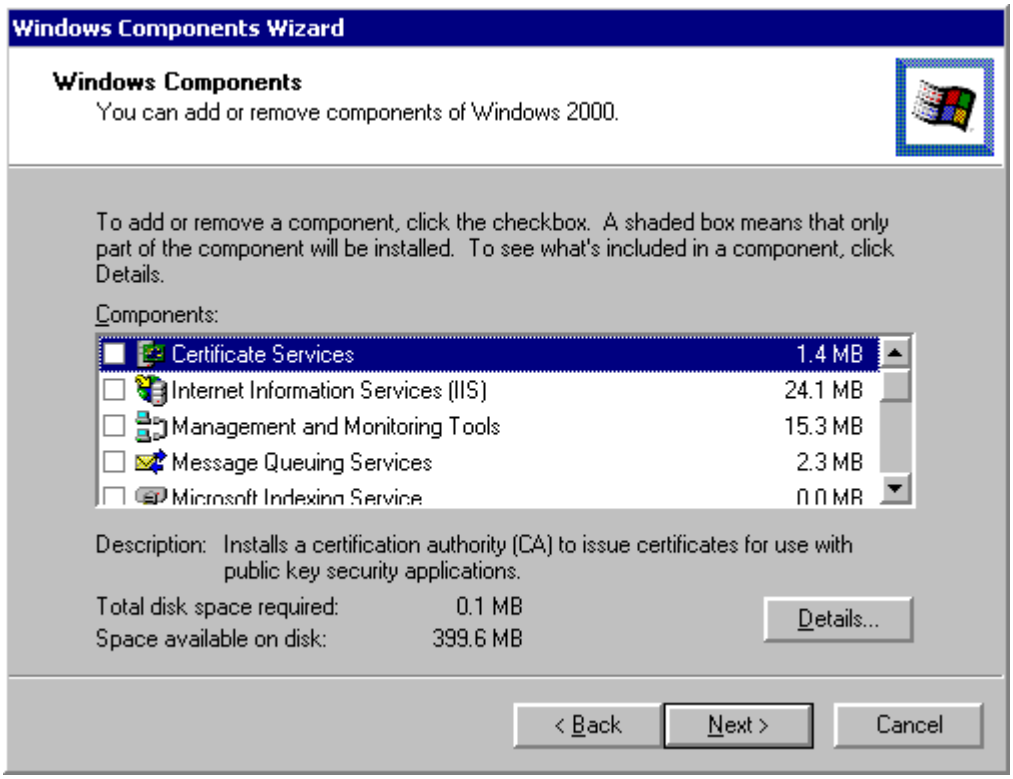


图 15.3 添加组件服务向导

如果是从 Windows NT Server 4.0 升级，应在升级后选中这些服务的配置，以便确保上一个操作系统中的服务能正常迁移。

终端服务

终端服务允许客户应用程序在服务器上运行，这样客户机可以作为终端而不作为独立系统运行。服务器提供多会话环境，运行客户机使用的基于 Windows 的程序。也可以使用“ Windows 组件向导 ”安装终端服务。有关终端服务的详细信息，参见本书的“ 部署终端服务 ”一章。

数据库服务器

Windows 2000 应用程序成员服务器为运行和管理诸如 SQL Server 之类的数据库软件提供稳定的操作平台。在安装 Windows 2000 Server 时，运行数据库服务不需要对操作系统进行更多配置。

如果您从 Windows NT 4.0 版或更早版本升级至 Windows 2000 Server，应确保在开始升级前备份成员服务器上的所有数据库。同时，如果您使用的数据库应用程序不是 SQL Server，应确保该数据库应用程序与 Windows 2000 Server 兼容。有关 SQL Server 的详细信息，参见 *Microsoft® BackOffice 4.5 Resource Kit* 中的“Microsoft® SQL Server™ Resource Guide”。

Web 服务器

Web 服务器是上面安装服务器软件的计算机，使用诸如超文本传输协议 (HTTP) 和文件传送协议 (FTP) 之类的 Internet 协议，响应 TCP/IP 网络上的 Web 客户请求。

以下是安装 Windows 2000 Web 成员服务器的一般要求:

- 查看 HCL 以确保硬件兼容。
- 确定哪些新的或附加组件适用于 Web 服务器。
- 备份数据，以防备升级或安装期间出现问题。
- 升级至 Windows 2000 Server 后测试 Web 成员服务器。

Internet 信息服务 (IIS) 是集成在 Windows 2000 Server 中的 Web 服务。可以使用 IIS 在企业 Intranet 上建立 Web 或 FTP 站点、建立 Internet 站点或开发基于组件的应用程序。

Windows 2000 Server 包含 Internet 服务管理器 Microsoft 管理控制台 (MMC) 管理单元。这个管理单元是一个强大的站点管理工具，能访问所有服务器设置。如果使用 IIS，就会使用这个管理单元管理企业 Intranet 上的复杂站点或在 Internet 上发布信息。

建议在升级至 Windows 2000 Server 后测试 Web 服务器。要验证从 Windows 2000 成员服务器到其它 Web 站点的连接是否正常，则应进行以下测试：

- 从服务器打开 Internet 服务管理器 MMC 管理单元，验证所有 Web 站点（升级前就存在）都已成功升级至 Windows 2000 成员服务器上的 Web 服务。验证服务能正常运行。
- 从客户机打开 Web 浏览器，验证 Windows 2000 成员服务器与 Web 站点的连接是否正常。

有关 IIS 的详细信息，参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide*。

代理服务器

Microsoft® Proxy Server 允许客户机和服务器访问 Internet,同时使 Intranet 免受黑客干扰。运行 Proxy Server 2.0 的成员服务器可以无缝升级，但为了让 Proxy Server 在升级后运行，还需要更新。

Windows 2000 Server 要求在成员服务器上安装 Windows 2000 Proxy Server 2.0 安装向导。要安装 Proxy Server，如图 15.4 所示，将安装向导下载在本地驱动器或软盘上，按向导说明操作。有关向导的详细信息，参见 Web 资源页的 Microsoft Proxy Server 链接，网址是：
http://windows.microsoft.com/windows2000/reskit/webresources。

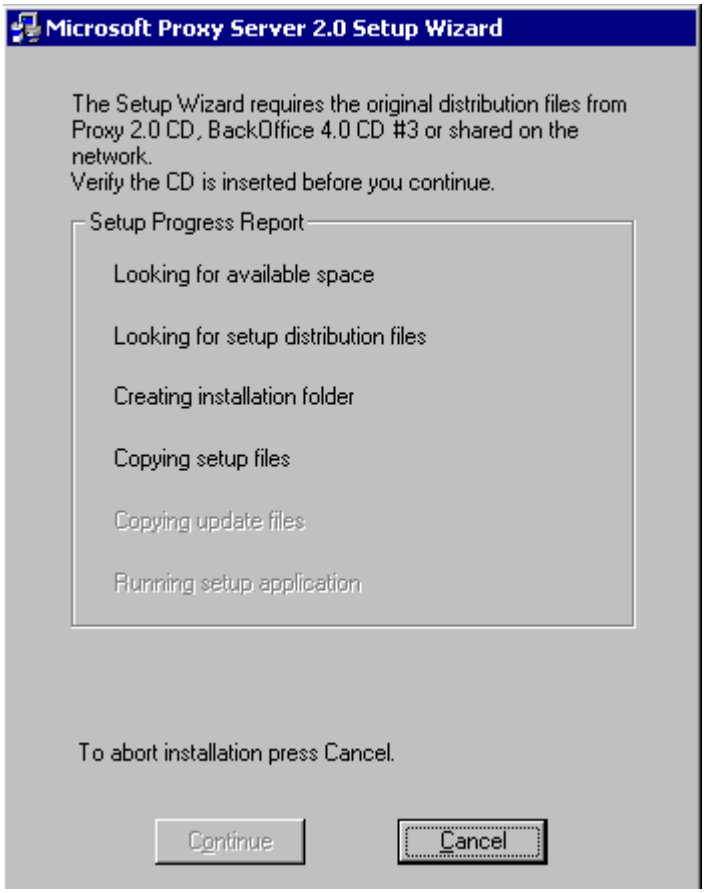


图 15.4　Proxy Server 2.0 安装向导

执行升级后和安装后任务

在将成员服务器集成到工作环境前，测试服务器以确保升级或安装成功非常重要。应确保 Windows 2000 Server 进入工作环境前，已准备好提供更好的服务和更多功能而不会出现料想不到的停机。

测试网络连接

在升级或安装成员服务器后，应验证网络连接是否正常。如果在 TCP/IP 网络环境中失去了网络连接，应用下面的列表作为故障排除指南。

- 在新升级的 Windows 2000 Server 上使用 IPCONFIG 工具验证 TCP/IP 配置参数。这些参数包含 IP 地址、子网掩码和默认网关。

  在用 IPCONFIG 工具验证配置后，再用 PING 工具测试网络连接。PING 工具是用来测试 TCP/IP 配置并诊断连接故障的诊断工具。打开命令提示窗口，用 Ping 命令检查各项。

  - 检查 127.0.0.1（回送地址）这可以验证 TCP/IP 是否已正确安装并加载。
  - 检查本地主机的 IP 地址。这可以验证它是否已正确添加。
  - 检查默认网关的 IP 地址。验证默认网关的运行是否正常。

- 检查远端主机的 IP 地址。验证是否可以通过路由器通信。

调整网络服务器

在将 Windows 2000 成员服务器安装在网络上后，可能需要对一些成员服务器作性能调整。即使升级经过仔细规划，仍无法避免所有可能出现的问题，例如瓶颈。如出现系统问题，可以用性能工具中的 Windows 2000 Server 系统监视器管理单元内的计数器查找。可以监视处理器、磁盘和网络活动以便收集数据。数据可以说明，对某些资源的需求导致的瓶颈意味着需要调整。

以下因素可能会导致瓶颈：

- 处理器、内存或硬盘等资源不足。

  可以列出网络硬件清单，确定哪些服务器需要升级硬件，以便将这一问题加以解决。

- 工作负荷不平衡，造成服务器负荷不均匀。

  为解决这些问题，Microsoft® Windows® 2000 Advanced Server 提供了网络负载平衡，以确保工作负荷在各资源间均匀分布。有关网络负载平衡和 Microsoft Advanced Server 的详细信息，参见本书的“确保应用程序和服务的可用性”。

在调整网络服务器时，应记住以下建议：

- 每次只做一个更改，因为看起来是由单个资源设置或组件引起的问题事实上可能是多个资源设置或组引起的问题。同时，对单个设置或组件反复更改要比对多个设置的反复更改更容易，一次更改的设置太多可能会使情况更糟。作一份更改以及更改对系统产生何种影响的记录。
- 每次更改后重复监视，以评估这些更改对服务器是否有积极影响。
- 检查“管理工具”中的“事件日志”查看器，看是否有性能问题产生的事件日志。

系统管理工具

使用 Microsoft 管理控制台 (MMC) 和相关管理单元执行 Windows 2000 Server 的大部分系统管理。

表 15.2 列出了文件、打印和 Web 服务的常见管理任务。

表 15.2 常见管理任务

任务	Windows 2000 Server 工具
管理文件共享	计算机管理 MMC 管理单元 Windows 资源管理器
管理打印机共享	打印机文件夹（在“控制面板”或“开始”菜单上的“设置”下）
管理 Web 站点	Internet 服务管理器 MMC 管理单元

执行远程管理的工具包含在 Windows 2000 Server 中。这些工具允许您从任何运行 Windows 2000 Server 的计算机远程管理服务器。

有关如何使用远程管理的详细信息，参见 Windows 2000 Server 帮助。

成员服务器规划任务列表

表 15.3 列出了规划成员服务器升级或安装时需要执行的任务。

成员服务器规划任务列表

任务	在本章中的位置
制定升级/安装规划和日程安排	成员服务器升级和安装规划
盘点现有硬件	为成员服务器升级或新安装做准备
确定系统要求	为成员服务器升级或新安装做准备
确定现有软件的兼容性和可靠性	为成员服务器升级或新安装做准备
确定第三方软件的兼容性	为成员服务器升级或新安装做准备
升级现有服务器	进行升级或安装
执行新安装	进行升级或安装
确定服务器角色： 文件服务器 打印服务器 应用程序服务器 Web 服务器 代理服务器	确定每台 Windows 2000 Server 的服务器角色
测试网络连接。	执行升级后和安装后任务
调整网络服务器性能	执行升级后和安装后任务

第 16 章 - 部署终端服务

终端服务可使客户计算机访问 Microsoft® Windows® 2000 和最新的基于 Windows 的应用程序。利用终端服务，用户可通过任何被支持的客户机在任何地点访问其台式机和安装的应用程序。对于 IT 经理和系统管理员来说，若要想提高应用程序部署的灵活性，控制计算机管理费用，以及远程管理网络资源，就必须学习 Microsoft® Windows® 2000 Server 的这种内置功能。

在阅读本章之前，建议您先阅读本书的“ Windows 2000 部署规划简介 ”和“ 部署规划 ”两章。

本章内容

终端服务概述
制定终端服务部署规划
制定终端服务部署设计
为终端服务部署配置服务器
为客户机部署做准备
测试和先导测试规划
使用帮助中心和管理工具
终端服务部署规划任务列表

本章目标

本章将帮助您完成以下规划文档：

- 终端服务部署规划

终端服务概述

在 Windows 2000 Server 中运行的终端服务允许所有的客户应用程序执行、数据处理，以及数据存储在服务器上进行。它通过*终端仿真*软件提供到服务器台式机的远程访问。终端仿真软件可以在多种客户机硬件设备上运行，如个人计算机、基于 Windows CE 的掌上电脑 (H/PC) 或终端。术语“ 基于 Windows 的终端 (WBT) ”涵盖了一组瘦客户机终端设备，这些设备可以访问运行多用户 Windows 操作系统（如终端服务）的服务器。

利用终端服务，终端仿真软件将键击和鼠标操作发送到服务器。终端服务器在本地完成所有的数据操作，并将显示结果传回。这种方法实现了对服务器的远程控制和集中的应用程序管理，可以将服务器和客户机之间的网络带宽要求减到最低。

用户可以通过任何 TCP/IP 连接访问终端服务，包括远程访问、以太网、Internet、无线网、广域网 (WAN) 或虚拟专用网络 (VPN)。用户的使用只受到连接中最弱链接特性的限制，链接的安全取决于数据中心的 TCP/IP 部署。

终端服务为网络资源提供了远程管理，为远程地点的分支机构用户提供了相同的体验，也为基于文本的计算机上的业务线应用程序提供了图形界面。终端服务的一些优点包括：

允许从可能不是基于 Windows 的设备上使用 32 位基于 Windows 的应用程序，如：

- Windows for Workgroups 3.11 或更高版本
- 基于 Windows 的终端（Windows CE 设备）
- 基于 MS-DOS 的客户机

- UNIX 终端
- Macintosh

- 不是基于 Windows 的客户机要求使用第三方附件。
- 终端服务客户要求最少的磁盘空间、内存和配置。
- 简化对远程计算机和分支机构环境的支持。
- 提供集中的安全和管理。
- 对应用程序和现有的网络基础结构完全适用。

终端服务是 Windows 2000 的内置功能。可以以下面两种模式之一启动终端服务：

远程管理

远程管理给系统管理员提供一种强有力的方法，可通过任何 TCP/IP 连接对每个 Windows 2000 服务器进行远程管理。可以从网络上另一台计算机管理文件和打印共享、编辑注册表，或就如同您坐在控制台旁操作一样执行任何任务。可以使用远程管理模式管理与终端服务的应用程序服务器模式不兼容的服务器，如运行群集服务的服务器。有关 Windows 群集的详细信息，参见本书的“确保应用程序和服务的可用性”。

远程管理模式只安装终端服务的远程访问组件。它不安装应用程序共享组件。这意味着您可以用非常小的开销在任务关键的服务器中使用远程管理。终端服务最多允许两个并发远程管理连接。对于这些连接不要求额外的授权，您不需要许可证服务器。

应用程序服务器

在应用程序服务器模式下，可以从中心位置部署和管理应用程序，从而节约管理员开发和部署时间以及维护和升级所需要的时间和人力。应用程序在终端服务中部署之后，许多客户机可以连接 — 通过远程访问连接、局域网 (LAN)、或广域网 (WAN)，并且从许多不同类型的客户机连接。

可以直接在终端服务器上安装应用程序，或可以使用远程安装。例如，可以使用组策略和 Active Directory 将“Windows 安装程序”应用程序软件包发布到终端服务器或一组终端服务器。应用程序只可通过管理员以每台服务器为基础安装，并且只有当启用适当的组策略设置时才可。

终端服务不能将单个客户计算机的 IP 地址传递到应用程序。因为此信息是 Windows 群集所要求的，所以您不能在应用程序服务器模式下使用群集服务。

当将终端服务器部署为应用程序服务器时要求客户授权。每个客户计算机，无论连接终端服务器所用的协议是什么，都必须有“终端服务客户访问许可证”以及“Windows 2000 客户访问许可证”。

终端服务授权组件

终端服务有其自己的为登录到终端服务器的客户机授权的方法，该方法与给 Windows 2000 Server 客户机授权的方法不同。终端服务授权包括以下几个组件：Microsoft Clearinghouse、许可证服务器、终端服务器以及客户许可证。

Microsoft Clearinghouse

Microsoft Clearinghouse 是 Microsoft 维护的数据库，用以激活许可证服务器并给发出请求的许可证服务器颁发客户许可证密钥包。Clearinghouse 储存关于所有激活的许可证服务器以及颁发的客户许可证密钥

包的信息。可通过终端服务授权功能的授权向导访问 Clearinghouse。

许可证服务器

许可证服务器储存为终端服务器安装的所有终端服务客户许可证并跟踪颁发给客户计算机或终端的许可证。在给客户机颁发许可证之前，终端服务器必须能够连接到激活的许可证服务器。一个激活的许可证服务器可以同时服务好几个终端服务器。

终端服务器

终端服务器是在上面启用终端服务的计算机。它为客户机提供到完全在服务器上运行的基于 Windows 的应用程序的访问并支持服务器上的多个客户会话。当客户机登录到终端服务器时，服务器会验证客户许可证。如果客户机没有许可证，终端服务器从许可证服务器为客户机申请一个。

客户许可证

每个连接到终端服务器的客户计算机或终端必须具有有效的客户许可证。客户许可证本地储存并在每次客户机连接到服务器时呈递给终端服务器。服务器验证许可证，然后允许客户连接。

图 16.1 是终端服务授权组件的示意图。

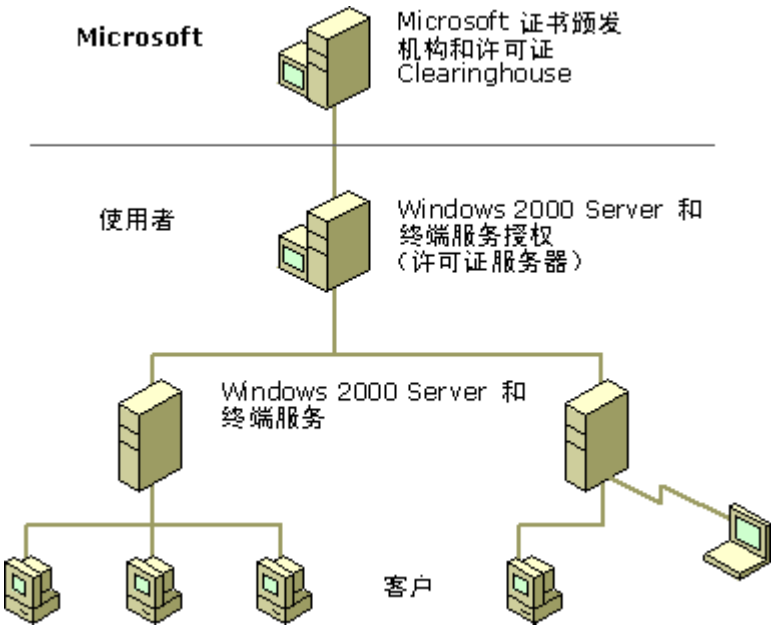


图 16.1 终端服务授权组件

有关安装终端服务授权组件的详细信息，参见在本章稍后的“ 安装许可证服务器 ”。

要求的许可证

在网络中部署终端服务和终端服务客户要求以下几个许可证：

Windows 2000 Server 许可证 此许可证包括在购买的产品中。

Windows 2000 Server 客户访问许可证 每个连接到 Windows 2000 Server 的设备都需要此许可证。客户访

问许可证允许客户使用 Windows 2000 Server 提供的文件、打印、和其它网络服务。Windows 2000 Server 的终端服务组件要求为 Windows 2000 Server 客户访问许可证提供“每客户”授权，除非您购买 Windows 2000 终端服务 Internet 连接程序授权。Internet 连接程序许可证在本章稍后介绍。

每个客户计算机或终端都要求以下几个许可证：

Windows 2000 终端服务客户访问许可证或 Windows 2000 许可证 客户访问许可证为每个客户计算机或基于 Windows 的终端提供访问 Windows 2000 Server 上终端服务的合法权限。例如，要求这种许可证启动终端会话并在服务器上运行基于 Windows 的应用程序。Windows 2000 许可证允许安装 Windows 2000 操作系统，另外还提供访问 Windows 2000 Server 中的终端服务的合法权限。只有在远程管理模式下连接到终端服务器的客户机不需要终端服务器客户访问许可证。

可选终端服务许可证

除了所要求的终端服务许可证外，还有两种可选的许可证可用：Windows 2000 终端服务 Internet 连接程序许可证和 Work at Home（在家工作）Windows 2000 终端服务客户访问许可证。

Windows 2000 终端服务 Internet 连接程序许可证

若不用客户访问许可证，可以购买 Windows 2000 终端服务 Internet 连接程序许可证。这种许可证作为 Windows 2000 Server 的附件许可证分开购买。它最多允许 200 个并发用户通过 Internet 匿名连接到终端服务器。这对于想给 Internet 用户演示基于 Windows 软件的单位很有好处，因为没有必要将基于 Windows 的应用程序重新编写为 Web 应用程序。用这种许可证访问终端服务器的用户决不能是本单位的员工。

当您将 Internet 连接程序许可证用于具体的 Windows 2000 Server 时，终端服务只允许匿名客户访问。不能在同一 Windows 2000 Server 上将 Internet 连接程序许可证与其它类型的终端服务客户访问许可证一起使用。

Work at Home Windows 2000 终端服务客户访问许可证

对于想使用终端服务为他们的员工提供从家访问 Windows 2000 台式机和 32 位的基于 Windows 应用程序的单位，可通过 Microsoft 卷授权程序获得 Work at Home 终端服务客户访问许可证。如果购买 Windows 2000 Professional 或终端服务客户访问许可证，您可以另外购买一个 Work at Home Windows 2000 终端服务客户访问许可证。

第三方扩展程序

MetaFrame™ 是 Citrix Systems, Inc. 的用于 Windows 2000 终端服务的第三方附件。它集成 Citrix 独立计算体系结构 (ICA) 协议并提供扩展功能，可用于：

- 客户设备
- 网络连接
- 本地系统资源

MetaFrame 同时提供多种管理工具与 Windows 2000 终端服务一起使用。有关 MetaFrame 的详细信息，请与 Citrix Systems, Inc. 联系。

制定终端服务部署规划

在弄清了终端服务的功能和授权要求后，便可以开始终端服务部署的规划阶段了。本节帮助您搜集制定本单位的终端服务部署规划所需要的信息。

部署终端服务的过程

在开始部署终端服务的规划阶段，应考虑使用如图 16.2 所示的规划步骤。

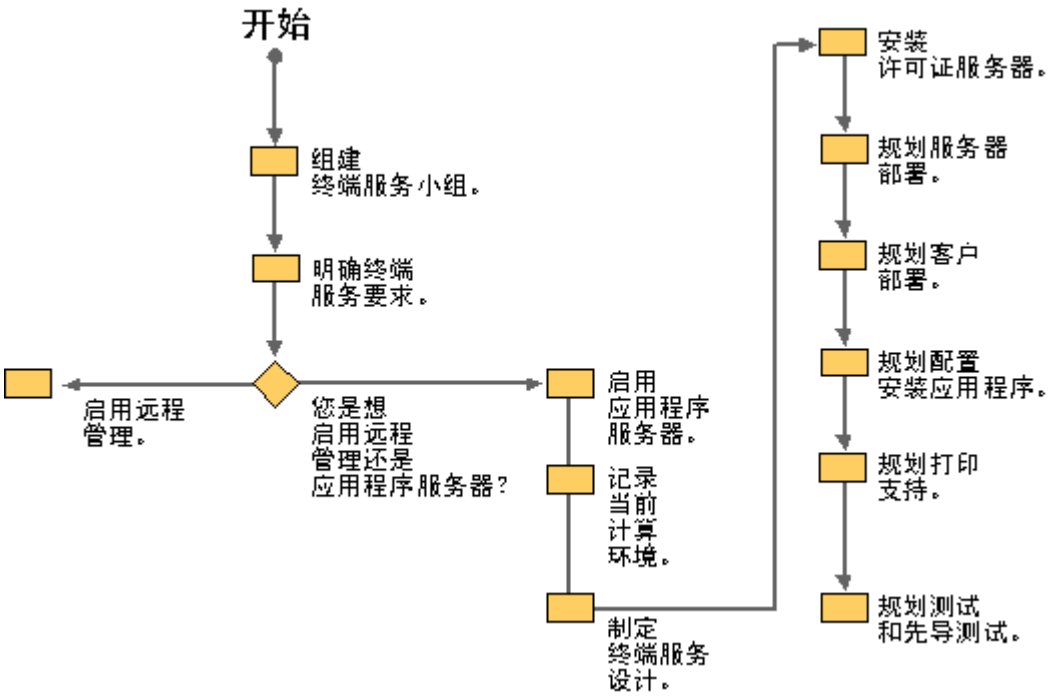


图 16.2 部署终端服务的过程

这些活动将在后面的几小节一一讨论。

组建终端服务小组

协作对终端服务的规划和部署至关重要。计划应包括负责网络问题的系统管理员，负责终端服务应用程序的管理员，以及负责业务单元的人员。

核心规划小组必须明确终端服务将针对的业务需求并设计终端服务部署。

明确终端服务要求

在小组组成之后，他们的首要任务是确定终端服务将针对什么业务方案。阅读本节业务方案有助于确定如何最好地利用本单位的终端服务。在开始规划部署之前，检查每个业务方案的要求。

方案 1：终端服务远程管理

终端服务远程管理使具有适当权限的系统管理员能够通过 TCP/IP 连接远程管理每个 Windows 2000 服务器。

在这种方案中，系统管理员使用 Microsoft 管理控制台 (MMC) 域管理器和目录服务管理等功能远程管理其目录域内的服务器。

通过启用远程管理模式下的终端服务，服务器管理扩展到目录林并进入混合模式域，在混合模式域中有 Windows 2000 和 Microsoft Windows NT 计算机两种。通过 Windows 群集，服务器管理可以扩展到群集服务器。如果所有的服务器都运行 Windows 2000，远程管理可以部署在企业内的每台服务器中，可实现直接连接和管理。

因为启用终端服务对服务器几乎没有影响，建议在目录林中的所有服务器上都启用终端服务。在这种情况下，如果一台服务器发生故障，另一台服务器便可接替它。对于混合环境，或必须包含控制的地方，远程管理可以部署在有限的服务器组中，如域控制器。其它服务器可以使用标准管理工具通过域进行管理。不论哪种情况，都可以从任何支持终端服务客户的平台进行管理，不一定是 Windows 2000。

在远程管理模式下，终端服务有两个内置“ 每服务器 ”连接，这种连接不要求特殊的安装和特殊的授权。

图 16.3 展示远程管理实现了跨目录林和在混合模式域中的服务器管理。

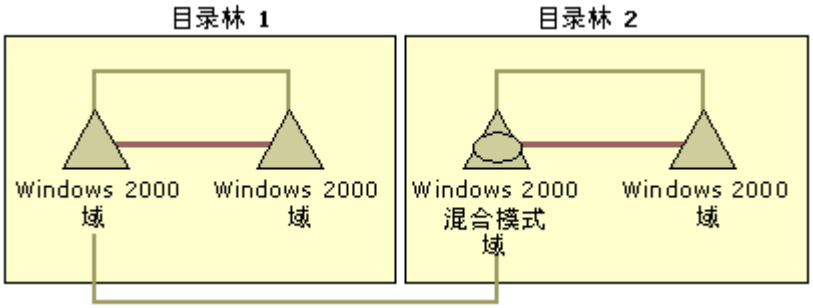


图 16.3 远程管理扩展服务器管理

方案 2：远程访问

远程访问通过外部 TCP/IP 连接扩展了终端服务的功能。用户的使用受连接中最弱的链接的特性限制。

在这种方案中，在计算机上安装了终端服务客户端软件的远程办公室的用户可以访问中心办公室里的终端服务器上的会计应用程序。可通过调制解调器进行远程访问连接，访问基本的公司数据。因为主要是键盘和显示信息在客户和服务器之间交换，带宽要求低，即使是使用很慢的调制解调器链接的用户也能得到很棒的效果。可以添加更多的应用程序，而不需要更多的带宽，只要这些应用程序不使用大量的图形。

在分支机构的某人可以访问网络资源之前，他们必须给出他们的凭据并接受完全身份验证。当通过终端服务器路由访问网络资源时，可以提供额外一层安全保护。

可采用一个类似的方法来访问很少使用的、已淘汰的或正在开发中的应用程序。

图 16.4 演示了远程办公室的员工使用 TCP/IP 连接连接到公司办公室的方法。

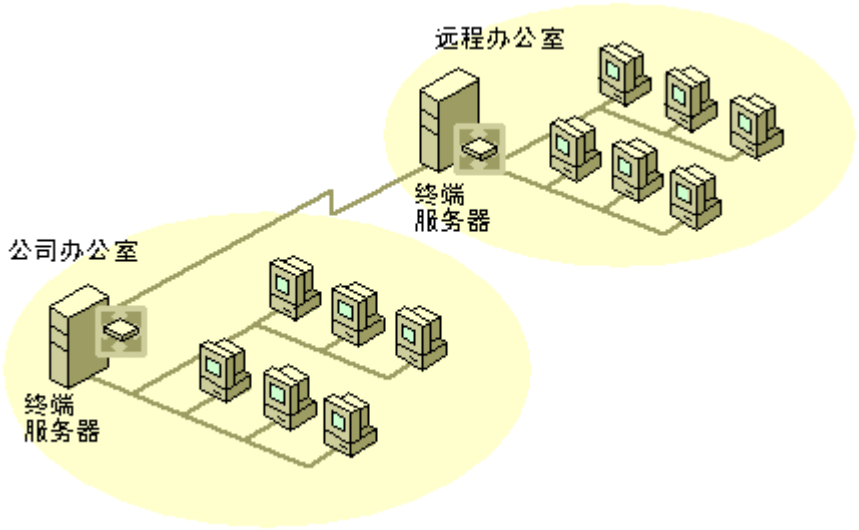


图 16.4 通过 TCP/IP 连接链接的公司和远程办公室

方案 3：业务线应用程序

终端服务的应用程序服务器模式对于部署业务线应用程序是很理想的，特别是那些安装起来很困难或必须经常更新的那些程序。

在这种方案中，数据输入操作员访问业务线应用程序，将产品信息输入到数据库中。因为应用程序在终端服务器上，数据输入操作员在基于 Windows 的终端上工作，而不是在客户计算机上工作。如果服务器发生故障，客户设备可以重新连接到另一台服务器。与终端服务器分开维护数据支持这种方案，通过一组终端服务器使用网络负载平衡可提供故障转移控制。如果终端发生故障，它可被在对数据输入操作员影响很小的情况下替换。

在整个单位内，各个部门的组织、安全的设计必须为每个用户执行的任务所要求的信息和网络资源提供适当的访问途径。

图 16.5 是数据输入操作员使用驻留在终端服务器上的业务应用程序将产品信息输入进数据库的方法。

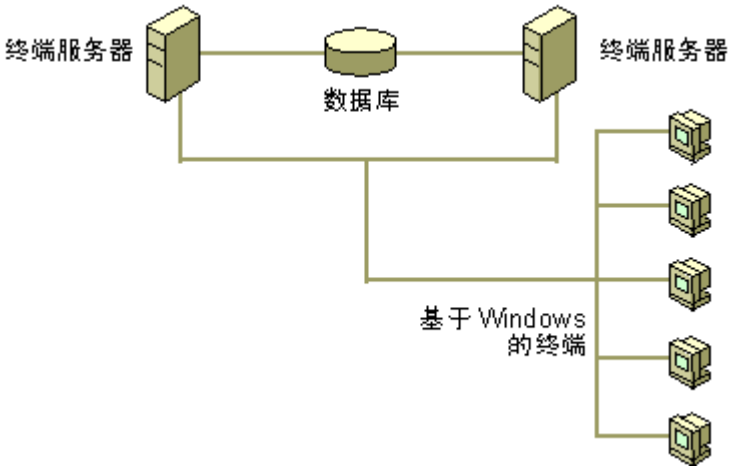


图 16.5 终端服务器上的业务线应用程序

方案 4：中央桌面部署

中央桌面部署通过在应用程序服务器模式下启用了终端服务的 Windows 2000 服务器中装载桌面应用程序实现。每个客户计算机都有单一、小型的应用程序，该应用程序允许模拟每个用户的基于 Windows 的桌面。应用程序实际上在服务器中运行。

在这种方案中，一个员工遍及全世界的全球性企业可以为其用户提供到生产和旧应用程序以及办公室效率工具的可靠访问。当启用了 Windows 2000 服务器中的终端服务后，即使是位于远程的或使用遗留硬件的客户机也可以运行受控制的，标准化的应用程序组。系统安全提供适当的访问客户机的权限。

因为所有用户都熟悉 Windows 桌面，开发人员可以使用如 Microsoft® Visual Basic® 等工具为专有的应用程序创建标准的基于 Windows 的用户界面。

图 16.6 演示了一个单位使用终端服务提供全球访问应用程序和工具的方法。

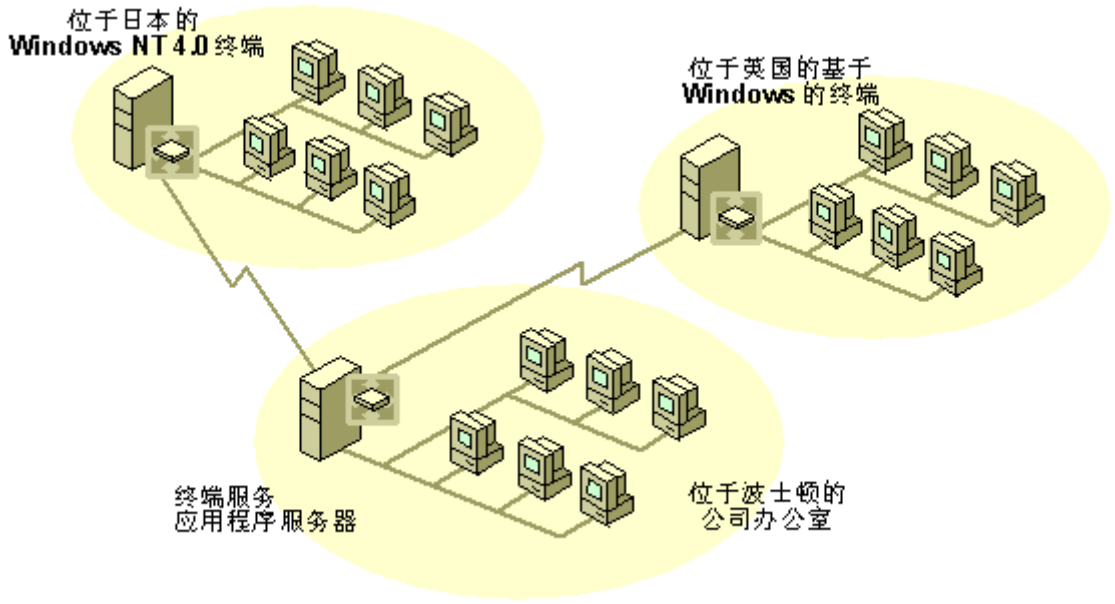


图 16.6 使用终端服务的应用程序和工具的中央桌面部署

部署要求

刚刚介绍的终端服务方案会常常重叠。例如，通过中央桌面访问他们自己台式机的用户有时也通过调制解调器进行远程访问。您在本单位部署终端服务以前，一定要认真研究表 16.1 中每个方案的要求。

表 16.1 部署要求

	远程管理	远程访问	业务线应用程序	中央桌面部署
授权		X	X	X
许可证服务器		X	X	X

域结构	X		X	X
负载平衡		X	X	X
漫游配置文件		X		
本地打印	X	X	X	X
安全性	X	X	X	X

准备计算环境

在设计终端服务部署之前，必须彻底了解当前的计算环境。有关记录计算环境的详细信息，参见本书的“部署规划”。有关具体到终端服务部署的信息，一定要考虑如下的注意事项。

在域控制器中安装许可证服务器

在 Windows 2000 域中，必须在域控制器中安装许可证服务器。在工作组或 Windows NT 4.0 域中，可以在任何 Windows 2000 服务器中安装域许可证服务器。然而，如果您计划从工作组或 Windows NT 域迁移到 Windows 2000 域，特别建议您在域控制器中或在可以升级到域控制器的计算机上安装许可证服务器。

通过广域网访问

确定路由器或防火墙上是否安装了防止客户机远程访问终端服务器的过滤器。检查以确保远程桌面协议 (RDP) 端口（端口 3389）在防火墙中没有被阻塞，并且到特定公司段的访问没有限制到网际协议 (IP) 或网际数据包交换 (IPX) 网络地址。如果有这些阻塞，而且它们阻止远程连接，工作人员必须在部署时解决它们。

访问网络服务

您可能给消费者或供应商提供使用应用程序或数据的权限，或您可能认为 Internet 是最终用户访问终端服务最便捷的方法。如果您计划使服务器通过 Internet 可用，应考虑对安全的影响。

如果本单位使用防火墙，确定它是数据包级的还是应用程序级的防火墙。数据包级的防火墙对于新协议较容易配置。如果本单位使用应用程序级的防火墙，检查一下供应商是否为 RDP 定义了过滤器，如果没有，与供应商联系并要求它们创建过滤器。

记录下网络连接到 Internet 所使用的方法。这有助于确定有多少带宽可用于终端服务。网络是否有永久连接？描述用于连接的线路的数量和类型，如 T1 或综合业务数字网 (ISDN)。

连接终端服务客户机和服务器

RDP 支持终端服务客户机和服务器之间的 TCP/IP 连接。该连接可以通过在本地 LAN 上的网络和拨号连接，或通过广域 VPN 连接。终端服务使用您提供的任何 IP 连接。然而，考虑下面的一点很重要，即您提供的连接的类型是否适合所做的工作；以及它提供的安全是否适合要传输的数据。单个用户可以通过低带宽调制解调器线路拨号，并实现很好的性能，但如果一个 100 人的办公室共享 28.8K 的线路就不合适了。

访问当前环境

对当前环境进行相当高水平的评估，包括基于 Windows 的终端、客户计算机、绿色屏幕终端、Macintosh 计算机、UNIX 工作站、UNIX X 终端，以及较大的掌上设备。不需记录个别计算机，估计数量并描述部门范围内的或单位范围内的标准就足够了。进行这项评估的任务包括以下几个：

- 提供当前正在使用的客户计算机的大约总数。
- 描述将运行终端服务器客户的计算机的当前配置，如 CPU、操作系统、可用的硬盘空间、RAM、以及显卡情况。记录现有的任何正式的或非正式的部门或单位标准，记下任何低于标准的计算机。任何达不到最低标准的客户计算机必须升级或更换。考虑拥有的每一类客户机的数量，确定最大化性价比的标准。
- 记录您的环境中有多少和哪些类型的终端，包括所有现有的将与终端服务一起使用的基于 Windows 的终端，以及所有绿色屏幕或必须更换的 UNIX X 终端。

  绿色屏幕终端不能用作终端服务器客户，在一些情况下可以将它们用于遗留大型机访问，或可以选择升级到基于 Windows 的终端以及具有终端服务和大型机访问权。
- 记录终端服务器客户必须与其接口的任何系统。如果当前客户计算机通过非 Windows 2000 网关访问这些系统，必须安装新网关。确定本单位是否具有从 Windows 环境访问这些系统所需要的适当的许可证。

应用程序部署的注意事项

记录您打算部署到使用终端服务的客户计算机上的应用程序。一些应用程序的一些功能妨碍它们与终端服务一起工作或使它们性能很差。有鉴于此，必须指导用户在可行的情况下本地安装这些应用程序。必须特别明确下列事项：

- 要求特殊硬件才能运转的应用程序，如条形码扫描仪或读卡机。只有当这些设备以特定的方法连接到客户计算机或终端，即计算机将外设看作键盘类型的设备，才能将这些设备与终端服务客户一起使用。通过并口或串口或通过特殊的卡连接到本地计算机的外围设备当前不能被基于 RDP 的终端服务器客户机识别。
- 多媒体应用程序或具有非常大的图形输出的应用程序在终端服务下不能很好地运行。许多游戏属于这种类型，数据流媒体应用程序也是如此。

在其它情况下，应用程序能够运行但需要特殊的安装程序或执行脚本。通常，这些脚本补偿程序中的问题，如误用注册表或缺乏多用户文件存储支持。与应用程序开发人员联系，以获取终端服务脚本。有关本主题的详细信息，参见 Web 资源页的“Terminal Services Application Information”链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources .

如果自定义应用程序不是作为支持多用户的应用程序而编写的话，可能需要修改或支持脚本。有关创建脚本的详细信息，参见 Web 资源页上的“Terminal Services Creating Installation and Execution Scripts”链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources.

备注 非管理用户不能使用 Windows 安装程序技术在终端服务器上安装应用程序。

制定终端服务部署设计

在您明确业务需要并记录您的计算环境之后，便可以开始计划部署终端服务了。本节将有助于搜集制定本单

位的终端服务部署规划所需要的信息。

安装许可证服务器

当在应用程序服务器模式运行时，终端服务要求许可证服务器。终端服务许可证服务是一个低影响的服务，它储存颁发给终端服务器的客户许可证并跟踪颁发给客户计算机或终端的许可证。

许可证服务器必须通过 Microsoft Clearinghouse 激活并与客户访问许可证一起装载，以便从 Clearinghouse 分发。许可证服务器只有颁发新许可证时才由终端服务器访问，对其的管理只涉及到从 Clearinghouse 获得许可证。

启用许可证服务器

可以在运行 Windows 2000 Server 安装程序时在计算机上启用终端服务许可证服务。建议在一个成员服务器或独立服务器上启用终端服务，在另一台计算机上安装许可证服务器。

有两种类型的许可证服务器，一种是域许可证服务器，另一种是企业许可证服务器。在安装许可证服务器之前，应考虑需要哪种类型的许可证服务器。

- 如果您想为每个域维护一个单独的许可证服务器，那么适合选用域许可证服务器。如果您有工作组或 Windows NT 4.0 域，那么域许可证服务器是唯一可以安装的类型。终端服务器只有与许可证服务器在同一域时，才可访问域许可证服务器。默认情况下，许可证服务器安装为域许可证服务器。

- 企业许可证服务器可以在站点内的任何域中服务终端服务器，但域必须是 Windows 2000 域。它只可服务同一站点中的终端服务器。如果您有许多域，适合选用这类许可证服务器。企业许可证服务器只可使用“ 添加/删除程序 ”安装，而不是在 Windows 2000 安装时安装。

当决定在物理网络中何处部署许可证服务器时，应考虑终端服务器如何发现许可证服务器并与其通讯。在为 Window 2000 启用终端服务时，终端服务器将开始轮询域和 Windows 2000 Active Directory™，寻找许可证服务器（在工作组环境中，终端服务器将广播到同一子网内的工作组中的所有服务器）。

终端服务器每隔 15 分钟轮询一次，寻找域许可证服务器，并每隔一小时检查一次目录服务，寻找企业许可证服务器。如果找到域许可证服务器，终端服务器每隔两小时检查一次。如果终端服务器不能找到域许可证服务器，那么它每隔 15 分钟检查一次。如果找到企业许可证服务器，终端服务器每隔一小时检查一次目录服务。这些检查产生的网络通信量可以忽略。

备注 在 Windows 2000 域中，必须在域控制器中安装域许可证服务器。在工作组或 Windows NT 4.0 域中，可以在任何服务器中安装域许可证服务器。如果您计划最终从工作组或 Windows NT 域迁移到 Windows 2000 域，必须在可以升级到 Windows 2000 域控制器的计算机上安装许可证服务器。

为快速激活许可证服务器，并通过 Internet 访问 Microsoft Clearinghouse，应在能访问 Internet 的计算机上安装服务器。

必须在启用 Windows 2000 终端服务器后的 90 天内启用 Windows 2000 许可证服务器。如果在这个期限结束时没有在 Windows 2000 服务器上启用许可证服务，那么 Windows 2000 终端服务将不能工作。

激活许可证服务器

必须激活许可证服务器以便识别服务器并允许它给终端服务器颁发客户许可证。您可使用授权向导激活许可证服务器。

有四种方法激活许可证服务器：

- Internet
- 基于 Web
- 传真
- 电话

如果运行终端服务授权工具的计算机连接到 Internet，则 Internet 激活方法是最快而且最便捷的方法。授权向导将引导您到激活许可证服务器的安全的 Microsoft Internet 站点。当您激活许可证服务器时，Microsoft 给服务器提供一个数字证书，该证书确认服务器所有权和身份。使用这种证书，许可证服务器可以与 Microsoft 进行以后的事务处理并接收给终端服务器的客户访问许可证。

如果许可证服务器没有 Internet 连接但您能从另一台计算机的浏览器访问万维网，那么您可以通过基于 Web 的激活方法激活许可证服务器。授权向导将引导您到安全 Microsoft Web 站点获得许可证服务器所需的证书。

激活许可证服务器的另外一些方法包括将您的信息传真到或打电话到与您最近的客户支持中心 (CSC)。授权向导也带领您完成这些步骤。可以使用授权向导找到适当的电话或传真号码。如果您使用传真激活方法，您的申请确认会通过传真从 Microsoft 返回。如果您使用电话激活方法，您的申请会由客户支持代理通过电话完成。

您只需激活许可证服务器一次。在等待激活完成的过程中，许可证服务器可以颁发临时许可证给客户，允许他们使用终端服务器 90 天。

唯一标识许可证服务器的数字证书以许可证服务器 ID 的形式储存。将此编号的副本放在安全的位置。要在许可证服务器被激活之后查看此号码，突出显示许可证服务器并从“**查看**”菜单选择“**属性**”。将通信方法设置为万维网，并单击“**确定**”。然后从“**操作**”菜单选择“**安装许可证**”，并单击“**下一步**”。许可证服务器 ID 列在授权向导屏幕的中间。

安装许可证

终端服务许可证必须安装在许可证服务器中，以便启用 Internet 连接程序设置，或用于非 Windows 2000 客户永久访问 Windows 2000 终端服务器。为获得 Windows 2000 终端服务客户访问或 Internet 连接程序许可证，可通过标准软件购买方法购买。在购买之后，便可以使用授权向导安装许可证。

正如有四种方法激活许可证服务器那样，也有四种方法安装终端服务许可证。当安装许可证时，会询问您有关购买许可证的信息。该信息如下：

- 如果您通过 Microsoft Select 或 Enterprise Agreement 购买或将购买许可证，您应提供注册协议号。
- 如果您通过 Microsoft Open License 购买许可证，在 Open License Confirmation 时应提供 Open License 和授权编号。
- 如果您通过 Microsoft LicensePak 购买许可证，您应回答 25 个字符的许可证代码，它位于 Microsoft LicensePak 包装上。

在安装许可证之后，许可证服务器可以开始部署许可证。具有 90 天临时许可证的客户将在下次他们登录时被升级到终端服务客户访问许可证（除非安装的客户访问许可证的数量超过未用的临时许可证数量）。

使用终端服务授权管理工具

终端服务授权是为帮助您激活许可证服务器、安装客户访问许可证、和跟踪终端服务器的客户使用情况而设计的管理工具。这样，终端服务授权帮助系统管理员精确地掌握和部署终端服务客户访问和 Internet 连接程序许可证。

使用终端服务授权，可以在连接到许可证服务器之后执行以下几个任务：

- 激活许可证服务器。
- 安装客户许可证。
- 重新激活许可证服务器。
- 释放许可证服务器。
- 重复客户许可证的安装。

所有的这些任务都可使用授权向导完成。

除了完成这些任务，还可使用终端服务授权连接到网络中的任何许可证服务器，然后查看该服务器上有关许可证的信息。可以查看下列有用的授权信息：

- 安装的客户许可证密钥包列表。
- 每个客户许可证密钥包中的许可证的总数，以及每个密钥包中可用的和已颁发的许可证的数量。
- 计算机的名称和每个许可证颁发的日期。
- 计算机的名称以及每个颁发的临时许可证的到期日。

当从许可证服务器申请许可证的客户的数量超过您激活的许可证的数量时，会提醒您安装新许可证。提示在“事件查看器”的系统日志中作为事件出现。未用的临时许可证的数量可用于确定您最终将需要的客户访问许可证的数量。

备份许可证服务器

备份许可证服务器是很重要的，这是为了确保在万一系统发生故障的情况下很容易地恢复授权信息。备份必须定期进行，并必须至少包括系统状态，以及 Lserver 目录。默认路径是 %windir%\system32\Lserver。

在还原计算机时，授权服务必须运行。将数据库和系统状态还原到原始许可证服务器（具有相同 ID 的服务器）会还原所有历史和当前的许可证信息。如果将备份授权数据库还原到另一许可证服务器上，那么许可证服务器只还原已颁发许可证的历史信息。没有颁发的许可证不还原。然而，有关没有颁发的许可证的信息会记录到系统日志中，可以在“事件查看器”中查看。系统日志中的信息将包括没有还原的未颁发的许可证的数量和类型。要还原没有颁发的许可证，使用电话安装方法安装那些许可证。客户支持代理可以重新颁发丢失的许可证。

为终端服务器访问设计网络

在部署终端服务时必须考虑网络基础结构。在很大程度上，所涉及的问题都是一般的网络设计问题，但终端服务需要一些特殊的考虑。

终端服务不能将单个客户的 IP 地址传递到应用程序。要求每个用户都有唯一的 IP 地址的多用户应用程序

在终端服务环境下不能正常工作，因为每个用户都从服务器本身的 IP 地址发出。例如，某些防火墙和遗留主机使用客户机的 IP 地址确定安全和物理位置。也许需要改变计划以使用终端服务支持这些应用程序。

相反，认识到所有用户将共享给定终端服务器的相同 IP 连接是非常重要的。破坏、锁定、或独占资源的应用程序或服务会与服务器的正常运行相互干扰。

网络负载平衡和终端服务

网络负载平衡用于在两个或更多服务器之间分配工作。网络负载平衡将一组服务器表示为单个虚拟 IP 地址，并提供动态分配负载的机制。这在下面的环境中是非常有用的：如有大量的用户连接到装有业务线应用程序的服务器、或连接到保留会话不是特别重要的数据库中时。因为终端服务不适用于群集，负载平衡常常能为服务很大的用户组提供好的解决方案。

传统的负载平衡解决方案不能始终保证用户可重新连接到同一服务器。在业务线方案等情况下，很少或几乎没有有关会话的数据需要担心。在使用更复杂的桌面部署或远程访问的情况下，企业可决定不支持切断连接的会话，以降低资源要求和提高安全性。最后，也可以使用某些类型的负载平衡的属性以重新连接到同一终端服务器，从而保留会话。

保留会话与保留用户数据不同。在管理两个或更多终端服务器时，通过将用户数据和用户配置文件储存到终端服务器以外的地方，可允许用户连接到任何服务器并有适当的访问权限。然后服务器只需要查看这个公共存储区，查找用户配置文件和存储内容。对于用户来说，无论他们连接到哪个服务器，效果是相同的。

网络负载平衡为许多终端服务器提供了好的解决方案。网络负载平衡使用 IP 仿射性，如果会话断开，可使具有相同 IP 地址的用户重新连接到同一计算机。这就意味着如果用户没有更换计算机，网络负载平衡可用于会话恢复。即使使用了动态主机配置协议 (DHCP)，只要用户不在此期间从网络注销，其 IP 地址依然保持相同，。

域名系统 (DNS) 是负载平衡的替换策略。对于循环 DNS，单个名称记录可解析为几个 IP 地址，每个 IP 地址都有相应的复制的服务器。如果您使用 DNS，在运行终端服务的服务器上停用“ **会话断开** ”。因为客户机可以连接到任何服务器，它可以连接到一台与仍在运行切断会话的服务器不同的服务器。

有关网络负载平衡的详细信息，参见本书的“ 确保应用程序和服务的可用性 ”。

设计和安装域结构

设计网络还涉及在设想的 Windows 2000 基础结构内规划终端服务的位置。有三个主要的域结构方案可应用于终端服务安装：

不使用域结构。在没有域体系结构的情况下，用户在每个运行终端服务的 Windows 2000 服务器上都需要单独的帐户。这限制了可扩展性并使用户组的管理更加困难。

在现有的 Windows NT 4.0 域环境中实现 Windows 2000 终端服务。这个方案允许您利用 Windows 2000 终端服务的新功能，而不会影响生产环境。然而，切记使用这种方法时，Windows NT 4.0 域模型的现有安全帐户管理器 (SAM) 将起作用。管理员可以选择把终端服务特定的属性添加到用户帐户。这会将少量的信息（通常为 1 KB或更少）添加到域 SAM 数据库的用户项中。

利用 Windows 2000 Active Directory 基础结构。这个方案充分利用 Active Directory。它利用在其数据库中主持数千个用户的能力。它还能使您选择当连接到终端服务时，应用组策略控制用户效果。

当您定义 Active Directory 结构时，建议将终端服务器放在单独的部门 (OU)，与其它计算机分开，并不带用户。终端服务 OU 只需包含终端服务计算机，不需要其它用户或非终端服务机器对象。正如您可能以不

同于管理客户计算机的方式管理膝上型电脑那样，也要以不同的方式管理终端服务器。

使用 Windows 2000 用户配置文件或漫游用户配置文件

配置文件描述特定用户的 Windows 2000 配置，包括用户的环境和首选项设置。配置文件通常包含具体的用户信息，如安装的应用程序、桌面图标、和颜色选项。可以使用位于“ **用户属性** ”对话框中的“ **终端服务配置文件** ”选项卡中的配置文件，为具体用户配置终端服务特定的配置文件。

在某些情况下，已经给用户指定了 Windows 2000 配置文件。在下列情况下指定特定终端服务的配置文件给用户可能会很好：

- 每当用户通过 WAN 访问终端服务时。
- 如果管理员想给用户提供一个不同于用户自己桌面环境的会话。

每当用户登录到运行终端服务的服务器，服务器试图以下列顺序装载配置文件：

- 用户的特定终端服务配置文件
- 用户的 Windows 2000 漫游配置文件
- 用户的 Windows 2000 配置文件

漫游用户配置文件

漫游用户配置文件允许用户在不同的计算机之间移动时，能拥有相同的环境和首选项设置。配置文件信息缓存在终端服务器的本地硬盘驱动器上。在如下列一些情况下，建议用户注销之后删除此信息：

- 到终端服务的访问是由一组终端服务主机提供。
- 到终端服务的访问不经常发生，而且您想把使用的磁盘空间数量减到最少。

删除缓存配置文件的最有效的方法是将所有的终端服务主机放在 Windows 2000 Active Directory 容器中，并对它们应用一个特定的策略，以在注销时删除所有的缓存配置文件。

为帮助使用漫游用户配置文件，提前规划并明确它们储存在何处以及如何管理它们。首先，确定文件服务器或打印服务器上的位置，它们必须有足够空间储存配置文件并可让终端服务用户随时使用。其次，创建 Windows 2000 共享，用户可以具有读/写权限的访问。必须将配置文件储存在不同于用户主目录的网络位置。

为了在一组终端服务计算机上使用漫游配置文件，终端服务计算机的应用程序和操作系统配置必须完全相同，如 %systemroot% 的位置和所有应用程序的安装位置。否则，将不同的配置分进不同的 OU 并分别管理它们。

组策略

组策略是管理和控制环境中终端服务行为的有效机制。可使用组策略管理一组注册表值和文件权限，它们共同定义可用于 Active Directory 站点、域或部门 (OU) 的计算机资源。

组策略建立在基于注册表的值的基本功能上，包括安全设置、软件安装、登录/注销和启动/关闭脚本、文件部署和重定向特殊文件夹。组策略由 Active Directory 启用，它在下面各组中影响计算机和用户：本地计算机、站点、域、和 OU。

如果单位有相同用户既用终端服务，又用 Windows 2000 Professional,使用策略时要慎重。相同策略应用

于终端服务和 Windows 2000 Professional 中的用户会话（在终端服务应用程序服务器中被禁用的每用户应用程序管理除外）。在此情况下，必须通过将计算机放置在分别的 OU 中，来对运行终端服务的服务器应用不同的计算机策略组。

应用程序服务器模式下的终端服务器中的用户不能激活 Windows 安装程序以将缺失的组件添加到应用程序中。因此，当初次安装程序时将所有必要的组件都本地安装上非常重要。为此，可以使用变换文件 (.mst)。变换文件如同 .msi 文件包的修改版本，它告诉 Windows 安装程序哪些组件应本地安装。

访问应用程序的权限

管理员可以用下列方法控制用户对终端服务应用程序的访问：

强制配置文件

配置文件可以指定哪些应用程序用户可见。

系统策略

策略可以防止用户通过 Windows 资源管理器或“运行”命令打开应用程序。策略是基于域的，因此它们既影响用户自己的计算机，又影响其终端服务会话。

组策略首先对域应用用户策略，然后要么合并要么以计算机策略替换它们。这允许终端服务器改变或限制提供给用户的功能。

编写很差的策略阻止用户访问域内所有计算机上的程序，而不是只阻止访问终端服务。如果管理员执行一个基于用户 ID 或 Windows 2000 组的策略，那么在策略中指定的所有事项应用于那个用户或组，不管他们使用什么系统。例如，一个禁止会计用户运行 Microsoft® Word 的策略影响域中所有会计用户，不论他们使用终端服务还是只是他们的本地计算机。

使用主目录

规划在终端服务环境中使用主目录是很重要的，因为大多数的应用程序都必须安装具体的用户信息或为每个用户复制配置文件。要使用户配置文件大小合理（低于 2 MB），建议所有的终端服务用户都建有网络主目录和网络“My Documents”目录，在该目录中储存具体应用程序的信息。

默认时，Windows 2000 为每个用户定义主目录。默认用户目录在文档和设置目录下。此目录包含用户文档和设置。用户文档储存在用户的主目录或“My Documents”文件夹中。终端服务将特定用户的应用程序文件（如 .ini 文件）写到用户的 Windows 目录，默认时将把位于系统 Windows 目录的任何应用程序写到用户的 Windows 目录。

用户通常使用他们的主目录保存他们的个人文件。如果漫游配置文件正被使用，但是主目录却位于用户的配置文件目录内，这可能会是个问题。每次用户登录时，Windows 2000 将用户配置文件目录中的所有内容都复制到配置文件缓存中。这会需要相当多的时间和资源，特别是在漫游配置文件通过网络储存时。

建议使用特定终端服务的主目录，它通过 MMC 管理单元自动可用。另一方法是在文件服务器上创建名为 Homedirs 的目录并赋予每个人“更改”权限。然后将终端服务主目录位置指定为 p:\Homedirs\%username%。终端服务自动创建用户名子目录并给它适当的权限。默认时，每个用户有访问自己主目录的完全权限，管理员可以将文件复制进目录，但不能在那里读取或删除文件。

所有用户的主目录重定向指向的虚拟驱动器号保持相同是很有益的，这样有助于使用应用程序兼容脚本。第一次在服务器上运行应用程序兼容性脚本时，它提示您设置指向用户主目录的根目录的驱动器号。这个驱动器号将用于所有以后的应用程序兼容性脚本。在同一服务器范围内的所有终端服务器使用相同的驱动器号是

很重要的。

文件夹重定向是 Windows 2000 的独有功能，该功能允许用户和管理员将文件夹的路径重定向到一个新的位置。新位置可以是本地计算机的文件夹，或者网络共享中的目录。用户能够在一个安全的服务器使用共享文档，如同这些文档就基于本地驱动器似的。使用此选项，管理员可以将用户的“ My Documents ”文件夹重定向到专用服务器共享，这样用户可以从自己的 Windows 2000 Professional 客户计算机或终端服务会话中访问。本功能使用组策略管理。

规划安全

安全是终端服务部署规划的重要组成部分。除了在 Windows 2000 部署规划应解决的安全问题外，终端服务有几个针对多用户环境的注意事项。

本节将讨论有关终端服务的安全问题，包括用于 Windows 2000 的 NTFS 文件系统的版本、用户和管理员权限、自动登录步骤、加密、和其它安全注意事项。

有关 Windows 2000 安全的详细信息，参见本书的“ 规划分布式安全 ”。

NTFS 文件系统

因为终端服务的多用户性质，强烈建议您使用 NTFS 的 Windows 2000 版本作为服务器的唯一的文件系统，而不要使用文件分配表 (FAT)。FAT 不提供任何用户和目录安全，而用 NTFS 可以将子目录限制给某些用户或用户组使用。这在象终端服务这样的多用户系统中至关重要。若没有 NTFS 提供的安全，任何用户都有权访问终端服务器中的每个目录和文件。

用户权限

终端服务以默认用户权限组分发，可以修改这些用户权限以提高安全性。为了登录到终端服务器，用户必须具有那台计算机的本地登录权限。默认时，远程管理模式下的终端服务器只赋予管理员访问计算机的权限，而在应用程序共享模式下赋予用户组的所有成员访问权限。因为 Windows 2000 默认时包括不是域控制器的计算机中用户组的所有域用户，所以所有域用户都能够登录到提供应用程序共享的终端服务器。允许登录的组和用户，以及给予他们的控制，可以通过终端服务配置功能加以改变。

被赋予通过如 RDP 协议访问权限的用户，以及可交互式登录到支持终端服务的服务器的用户被自动包括在内置终端服务用户本地组。在用户交互式登录到终端服务器时用户只属于这个组。这个内部组给予管理员控制终端服务用户可以访问的资源的权限。这个组类似于内置交互式组。

避免将终端服务配置为域控制器，因为应用于此类服务器的任何用户权限策略会应用到域中的全部域控制器。例如，要使用终端服务，必须授权用户在本地登录。如果运行终端服务的服务器是域控制器，用户将能够本地登录到终端服务域的所有域控制器中。

管理员权限

终端服务器中管理员组的成员有控制哪些用户有访问权限、具有何种权限、以及可运行的应用程序的权限。这种控制的大多数是管理员在 Windows 2000 服务器中通常权限的一部分。这些权限在终端服务下得以扩展到：

- 服务器管理 - 使用终端服务配置工具设置用户权限和会话活动以及断开操作和会话功能。
- 用户控制 - 通过终端服务配置设置用户使用终端服务的权限。通过用户管理器扩展程序设置终端服务的配置文件信息。

- 会话控制 - 使用终端服务管理器功能监视活动用户、会话、和进程，映象会话，或强迫断开。
- 应用程序安装 - 当在应用程序共享模式下运行时，只有管理员可以在终端服务器上安装应用程序。这种限制不适用于远程管理。

自动登录步骤

视人们使用终端服务的情况，可以赋予他们访问文件系统的权限。只需要访问单个应用程序（如某数据库）的用户可以在启动时直接运行应用程序。这可通过客户连接管理器配置终端服务器客户，自动为用户启动具体应用程序来完成。一个预先配置的终端服务器客户可以发行到组内的一组用户，让他们也一样可直接调用应用程序。如果终端服务器将用于把单个应用程序提供给允许连接的任何人，服务器可以配置为在登录时自动启动那个应用程序。这使用终端服务配置来完成。

还可以允许用户不用输入用户名和密码就可连接。还可以通过客户连接管理器以每用户为基础、或通过终端服务配置以每服务器为基础、或者用户管理器扩展程序来完成。通常，只有当用户直接登录到业务线应用程序，特别是当应用程序本身要求密码才能访问时，才需计划使用这种连接方法。使用这种服务器功能要慎重，因为这意味着具有终端服务客户的任何人都可以登录到服务器。

Windows 2000 提供辅助登录功能。这种功能主要用于允许用户在不同的安全环境设置下调用应用程序。这在终端服务环境中很重要，在这种环境中客户计算机自动以基本用户帐户登录，而当前用户想执行要求更高安全级别的应用程序。在这种情况下，可以使用 **runas** 命令在不同的环境下启动应用程序，而不必注销用户。

可以在命令提示符下输入 **runas** 命令或者可以加入一个应用程序快捷方式。在创建应用程序的快捷方式之后，**runas** 功能可以很容易地加入进来：选择快捷方式的“ **属性** ”选项中的“ **作为不同用户运行** ”。在执行应用程序之前，提示用户输入 Windows 2000 域用户帐户和密码。

编辑用户特定的信息

当用户登录到系统时，终端服务执行 System 32 目录中的名为 UsrLogon.cmd 批处理文件。这种文件对用户环境进行任何必要的修改，并确保用户可以正常运行他们的应用程序。如果对用户环境的终端服务修改必要，可以通过编辑此文件进行修改。要注意到编辑此文件可能会与应用程序兼容性脚本产生问题，因为该脚本从此批处理文件中执行。

更改登录过程

在登录脚本中，应检查是否有环境变量 %CLIENTNAME% 或者 %SESSIONNAME%。这些环境变量是针对终端服务的，只当用户登录到终端服务器（处于远程管理或应用程序服务器模式）时才出现在他们的环境中。例如，如果脚本确定反病毒软件是在终端服务上运行，可以选择不执行它。

加密

可用三个不同的加密级别进行终端服务客户和服务器之间的数据传输。注意高级加密只有在北美才有。

低级加密

使用低级加密时，从客户到服务器的通信使用 RC4 算法和 56 位密钥（RDP 4.0 客户采用 40 位密钥）加密，而从服务器到客户的通信不加密。低级加密保护敏感的数据（如密码项和应用数据）。从服务器发送到客户机的数据是以屏幕刷新进行的，即使当未加密时也很难截获。

中级加密

使用中级加密时，两个方向的通信都是使用 RC4 算法和 56 位密钥（RDP 4.0 客户机采用 40 位密钥）加密。

高级加密

两个方向的通信都使用 RC4 算法和 128 位密钥加密，只用于北美版本的终端服务中。在终端服务的出口版本中，高级加密使用 RC4 和 56 位密钥（RDP 4.0 客户采用 40 位）。

其它安全注意事项

当规划终端服务安全时，应考虑下列事项：

智能卡

Windows 2000 交互式登录能够使用与私钥一起储存在智能卡中的 X.509 版本 3 证书验证使用 Active Directory 网络的用户身份。然而，这种功能不可用于通过终端服务的用户身份验证。这还可应用于其它基于硬件的身份验证设备。

网络和通信安全　远程访问不限制对终端服务用户的访问，因此如果一个用户与 Internet 或另一个系统建立调制解调器或 VPN 链接，终端服务上的每个用户都有权访问该链接。

终端服务上的信息服务　必须停用匿名文件传输协议（FTP）以防止对文件系统的不安全访问。

删除未使用的服务　删除 IBM OS/2 和 POSIX 子系统可防止用户执行违反安全规章的 OS/2 或 POSIX 应用程序。有关保证系统安全的详细信息，参见本书的“规划分布式安全”。

远程访问

终端服务能让远程用户访问那些通过低性能拨号或很慢的 WAN 连接无法使用的应用程序。终端服务发送的屏幕、鼠标、和键盘信息通常比下载应用程序然后在远程用户的计算机本地运行所使用的带宽少。

Internet 上的终端服务

用户还可以利用第二层隧道协议（L2TP）或点对点隧道协议（PPTP）通过 Internet 访问终端服务。通过使用加密，无论哪种隧道选项都为在公众媒体上进行操作的用户提供对专用网络的安全访问。建议使用这些协议因为它们能提供安全保证，其实终端服务可以通过任何 TCP/IP 连接访问。

防火墙

如果本单位使用防火墙保证安全，记住要让端口 3389 保持打开以便在客户机和服务器之间进行 RDP 连接。为使效果最佳，要使用采用基于用户身份验证的防火墙。如果运行终端服务的服务器的 IP 地址已经得到访问权限，那么基于 IP 地址赋予访问权限的防火墙允许用户通过。

为终端服务部署配置服务器

建议您为终端服务购买的服务器要从同一个供应商那里购买并且以同样的方式配置它们。这将有助于管理终端服务。如果您部署终端服务是为了满足不同的需要，应考虑根据不同的功能将服务器分进几个组并使每个组的服务器尽可能类似。

如果本单位有设备标准，当规划采购新硬件以满足终端服务需要时应遵循这些标准。如果有必要，按照比现在更高的标准，以使硬件和软件的管理和维护尽可能简单。

当规划服务器部署时，应考虑内存、页面和转储文件、CPU 和注册表。“ 转储文件 ”在万一发生故障时用于内存转储。每一项的注意事项如下：

内存

一项好的原则是基本操作系统服务用 128 MB RAM，再加上每用户所需的额外的量。这个额外的量有所变化，每一会话应该需要 16 MB 到 20 MB 的内存。在估计这个额外的量时，用户桌面大致需要 13 MB，然后加上运行应用程序所需要的量。注意当几个用户运行同一应用程序时，应用程序的代码不复制到内存中（可执行的程序代码通过应用程序的实例共享）。16 位的应用程序大约比 32 位应用程序需要的内存多 25%。

如果用户运行内存开销大的应用程序（如占用大量内存的客户/服务器应用程序），必须增加分配给每个用户的 RAM 的量。每台服务器需要有足够的物理内存以确保几乎不需使用页面文件。

页面和转储文件

分配给每台服务器页面文件的磁盘空间必须至少为物理 RAM 的总量的一倍半。

将终端服务器操作系统放在一个物理驱动器上，而把页面文件指定到另一个物理驱动器上是一个好主意。如果服务器有大量的物理内存，必须考虑硬盘驱动器空间是否足够用来记录系统分区中的转储文件。应考虑此类因素，如：总的内存空间、页面文件大小、安装的应用程序、以及总的硬盘驱动器的大小。为使性能更佳，页面文件必须在分开的物理磁盘上。应考虑停用大 RAM（通常 128 MB 或更大）系统的转储文件，除非驱动器 C 足够大到可以保存转储文件。

CPU

终端服务器必须符合 Windows 2000 Server 的要求。每用户所要求的处理的量取决于运行的应用程序的类型。这最好通过试验部署确定。有关确定规模的详细信息，参见 Web 资源页中“ Terminal Services Scaling ”链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources .

注册表

注册表大小在安装时动态设置并基于页面文件大小而定。注册表配额基于内存大小。注册表大小还可以从“ 控制面板 ”设置。双击“ **系统** ”，然后单击“ **高级** ”选项卡。在“ **高级** ”选项卡上，单击“ **性能选项** ”，然后单击“ **更改** ”。输入注册表大小。

为客户机部署做准备

客户计算机或终端使用安装在磁盘或固件上的小型客户程序连接到终端服务器。选择使用哪一种客户平台取决于当前的安装基础和单个用户的需要。至少，要确保每个您希望连接到终端服务器的客户计算机或终端在物理上应能够主持客户端软件和通过网络连接。

部署到基于 Windows CE 的终端

基于 Windows CE 的终端通常是最“ 像 Windows ”的可以用来访问终端服务的终端。这些终端使用向导来安装和配置，向导运行的是 Microsoft® Win32® 用户界面，大家已在 Microsoft® Windows® 95 或更高版本的基于 Windows 的操作系统中很熟悉这种界面了。

应考虑从提供使管理员能远程执行终端升级、终端配置、和资产管理的工具的供应商那里购买终端。

基于 Windows 的终端通常可以本地配置，包括：

- 使用 DHCP
- 连接方式采用 LAN、点对点协议 (PPP)、IP 地址、子网掩码、或网关
- 当建立连接时启用 DNS 查找终端服务器名称

大多数基于 Windows 的终端都可通过使用 PPP 的拨号连接访问终端服务。注意一些基于 Windows 的终端在登录过程中不支持加密。在这种情况下，必须将给网络提供连接的设备配置为明文密码，否则不能建立连接。终端服务器上的会话登录始终是加密的。

基于 Windows CE 的终端可包括其它终端类型的模拟器作为固件的组成部分。此类终端的用户可以同时与不同类型的服务器建立连接并在终端设备上的不同模拟器之间变换。

在会话之间切换可以使用基于 Windows CE 的终端上的热键完成：

- CTRL+ALT+END — 将基于 Windows CE 的终端外壳 UI 送到前台。
- CTRL+ALT+UP ARROW — 切换到前面的活动会话，不用将外壳带到前台。
- CTRL+ALT+DOWN ARROW — 切换到下一个活动会话，不用将外壳送到前台。
- CTRL+ALT+HOME - 如果在运行，切换到默认连接。如果它未运行，外壳启动连接。
- F2 — 显示终端属性配置 UI。

有关提供基于 Windows CE 终端的供应商的详细信息，参见 Web 资源页中的“ Terminal Services Vendors ”链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources。

部署到客户计算机

连接到终端服务的基于 Windows 的客户计算机至少应有运行速度为 33 MHz的 80386 微处理器（但建议使用 486/66），16 位 VGA 显卡和 Microsoft TCP/IP 堆栈。终端服务客户运行于 Windows 2000、Windows for Workgroups 3.11、Windows 95、Windows 98、和 Windows NT 3.51 或更高版本。

终端服务客户只占用大约 500 KB 的磁盘空间，运行时通常使用大约 4 MB 的 RAM。如果启用客户机位图缓存，可能还要再使用 10 MB 的磁盘空间。为使性能达到最佳，运行终端服务客户的计算机应为 Windows for Workgroups 3.11 或 Windows 95 提供 8 MB 以上的物理 RAM，Windows 98 需 24 MB 以上，Windows 2000 需 32 MB 以上。

RDP 客户端软件现在默认安装为终端服务的子组件。默认时，各种客户程序安装在这个目录：

```
%systemroot%\system32\clients\tsclient
```

有两个选项部署客户：

- 创建文件共享通过网络安装。
- 从“ **管理工具** ”菜单选择“ **终端服务客户创建** ”并制作可以以软盘安装的客户映像。

备注 终端服务客户要求 TCP/IP 连接到服务器，但必要时终端服务可以使用 IPX 访问 Novell 服务器。

升级至终端服务

您升级到终端服务所采用的方法取决于现有的终端服务设置：

有或者没有 MetaFrame 的 WinFrame 没有从 WinFrame 直接升级到终端服务的路径。在这种情况下您首先必须升级到 Microsoft Terminal Server 4.0，然后升级到 Windows 2000。

没有 MetaFrame 的 Terminal Server 4.0 安装了 Terminal Server 4.0 之后，有直接升级到终端服务的路径。当您安装 Windows 2000 时，服务器识别 Terminal Server 4.0 版本，自动执行升级，并自动在应用程序服务器模式下启用终端服务。注意如果您在应用程序服务器模式下启用终端服务，必须重新安装现有的应用程序。

有 MetaFrame 的 Terminal Server 4.0 从有 MetaFrame 的 Terminal Services 4.0 升级类似于从 Terminal Server 4.0 升级，但首先必须升级到用于 Windows 2000 的 MetaFrame 版本。在 MetaFrame 升级之后，可以遵循从没有 MetaFrame 的 Terminal Server 4.0 升级相同的步骤。

没有终端服务的 Windows NT 当您安装 Windows 2000 时，在远程管理或应用程序模式下选择终端服务，以启用终端服务。

安装和配置应用程序

配置为在应用程序服务器模式下运行终端服务的 Windows 2000 服务器，可以提供到任何数量的应用程序的多个并发用户连接。

建议使用“ 控制面板 ”中的“ 添加/删除程序 ”功能添加或删除应用程序。这能自动管理终端服务安装要求。也可以直接安装应用程序，假定服务器通过使用“ **change user /install** ”命令行设置到安装模式。服务器可以用“ **change user /execute** ”切换出安装模式。

当使用“ 添加/删除程序 ”时不需要这些命令。因为使用命令行始终有发生错误或遗漏的可能性，最好通过“ 添加/删除程序 ”安装。如果应用程序没有使用“ 添加/删除 ”安装，也没有使用命令行设置安装模式，那么必须将该应用程序删除，然后重新正确安装。

只允许管理员在终端服务应用程序服务器上安装应用程序。

通过组策略部署应用程序

使用 Windows 安装程序通过 Active Directory 和组策略部署应用程序是一个非常灵活的应用程序部署方法。它允许以多种不同方法安装和管理应用程序。使用 Windows 安装程序部署应用程序的三个主要方法是：

- 用户在本地计算机上安装。
- 系统管理员从域控制器指定给用户或计算机。
- 系统管理员从域控制器发布给用户。

在使用 Windows 安装程序安装应用程序之前，必须为应用程序提供一个 .msi 安装软件包。

从域控制器部署应用程序

要从域控制器部署应用程序，系统管理员必须给计算机指定基于 .msi 的应用程序。应用程序服务器不能给用户指定或发布应用程序。

如果原始的应用程序安装软件包不能将应用程序的所有必要的组件安装到本地磁盘，则要求变换文件。变换文件允许您在安装时选择必须安装的组件。

系统管理员还可以从远程会话或应用程序服务器控制台安装应用程序。用下列命令启动典型安装：

```
Msiexec/I ApplicationName.MSITRANSFORMS=TransformFileName.MST ALLUSERS=1
```

在多用户环境下安装应用程序与安装到单个用户中大有不同。应用程序服务器软件安装决不能危害正在运行的系统，必须配置安装以允许并发用户。鉴于这些理由，只有管理员才能安装应用程序，而用户不能安装任何应用程序。

在允许远程用户连接之前，系统管理员应决定需要哪些应用程序，确保应用程序已在本地安装并可用。

支持多语种和国际用户

Windows 2000 多语种版本也提供终端服务。Windows 2000 多语种版本允许您在计算机上安装并配置多个用户界面语言。这样简化了部署过程并降低跨国机构的硬件费用。例如，一家瑞士公司，按照法律它应该提供给用户英语、法语、和德语界面，一台服务器就可以提供所有这三种语言。

在 Windows 2000 多语种版本中启用终端服务之前，应确定需要哪些用户界面语言。如果终端服务计算机为全世界的用户服务，但所有的国际用户都懂英语，就可以部署终端服务的国际英语版本。

管理员可以使用组策略设置用户界面语言。用户从“ 控制面板 ”的“ **区域选项** ”中的“ **常规** ”选项卡中选择他们的语言。当用户的漫游配置文件指定了一种没有安装的语言，系统默认为英语。

终端服务根据配置的时区跟踪时间，而不是根据单个用户的时间。位于与服务器不同时区的用户必须考虑时差因素。

从终端服务打印

从终端服务打印类似于从 Windows 2000 的其它版本打印。然而，用户和管理员必须注意某些重要差别。

在终端服务环境下有多种方法管理网络打印。在一个单位或部门的小组内，管理员可以在运行终端服务的服务器上本地配置打印机。可以通过并口或网络接口本地接上打印机。这些打印机自动可供所有系统用户使用。

想本地打印到连接到自己计算机上的用户可以选择要么使用终端服务客户功能将打印作业重定向到本地设备，要么使用对等网络。

用 RDP 协议打印到本地打印机

终端服务提供打印机重定向，可将打印作业从终端服务器路由到与客户连接的打印机。通过 RDP 有两个方法给客户提供到本地打印机的访问权限：自动打印机重定向和手动打印机重定向。

自动打印机重定向在所有的 Win32 客户机平台上受支持，包括 Windows 95、Windows 98、和 Windows NT。当客户机登录到终端服务时，自动检测到与 LPT、COM、和 USB 端口连接的本地打印机并在用户会话中创建相应的队列。当客户机断开或结束会话时，打印机队列被删除，所有等待的打印作业终止。

Windows for Workgroups 3.11 和 WBT 客户必须使用手动打印机重定向。在这种情况下，使用“ 控制面板 ”中的“ 添加打印机 ”向导手动添加打印机。使用客户计算机名称从可用的端口列表中选择打印机端口。可以使用终端服务连接配置基于“ 每连接 ”或使用 Active Directory “ 用户和计算机 ”或“ 本地用户和计算机 ”基于“ 每用户 ”禁用打印重定向。有关打印机重定向的详细信息，参见 Windows 2000 Server “ 帮助 ”。

网络共享打印机

如同本地磁盘驱动器一样，“ **网络共享** ”允许用户从服务器远程访问打印机。如果用户在本地打印机上安装网卡，它就变成网络打印机，就不一定需要在用户的计算机上启用文件共享。

打印机以每用户为基础定义，因此，在打印机为特别用户定义之后，在他们会话时，它只能供那个用户使用。另外，如果用户使用“ 打印管理器 ”，他们只能看到他们有权限用其打印的打印机。当用户注销时，服务器取消打印机重定向。另外，打印机重定向不可用于基于 MS-DOS 的应用程序。

“ **网络共享** ”方法是为与运行 Windows for Workgroups 3.11 或更高版本的个人计算机本地连接的打印机而设计的。执行 RDP 的 WBT 的用户目前不能使用这种方法打印到本地打印机。

通过 WAN 或拨号连接打印

如果用户通过 WAN 或拨号连接访问终端服务，要注意正确评估所有打印作业的带宽要求，因为这些工作要通过连接执行后台打印。

如果用户打印到本地打印机，该本地打印机驻留在用户的 LAN 但要通过运行终端服务的服务器的慢速链接，打印作业会通过慢速链接进行后台打印。这会增加终端服务的带宽要求，因为网络不但要处理击键、鼠标事件、和屏幕更新，还要处理打印通信。

同时建议您尽量少通过这些慢速链接打印大的图形或完成彩色打印作业，因为它们消耗相当多的带宽量。

客户机配置的最佳做法

可以通过如下这些建议做法使用户使用终端服务的效果达到最佳：

- 尽量少使用图形，包括动画、屏幕保护程序、闪烁光标、和动画 Microsoft Office 助手。
- 停用“ 活动桌面 ”。
- 停用平滑滚动。
- 尽量少使用图形和动画，如桌面上的层叠式菜单，特别是“ 开始 ”菜单。将快捷方式放在桌面，尽量减少“ 程序 ”子菜单。避免在墙纸中使用位图，在“ **背景** ”选项卡中在“ **显示属性** ”将“ **墙纸** ”设置为“ **无** ”，从“ **外观** ”选项卡中选择单色。
- 在客户计算机上启用文件共享，用很容易辨认的名称（如“ drivec”）共享驱动器。要注意涉及的安全问题。
- 应尽可能避免使用 MS-DOS 或 Win16（16 位）应用程序。
- 配置终端服务器，使其将用户的登录名称而不是计算机名返回到使用 NetBIOS 功能调用计算机名的的应用程序。
- 训练用户使用终端服务热键组合。终端服务客户会话中使用的热键组合与 Windows 2000 会话所使用的热键组合有一些重要区别。

测试和先导测试规划

发现终端服务部署中的潜在问题的最佳时机是在测试和先导测试期间。利用系统调整和查错的机会，可以暴

露出基础结构、系统配置、或软件方面的问题。

测试实验室的注意事项

检验终端服务器部署的理想环境是测试实验室，这种实验室尽可能地模拟实际的部署环境建造。测试实验室将作为本单位的微缩版本，使工作人员能在部署之前看到终端服务的工作情况。

当建立终端服务测试实验室时应考虑下列事项：

- 使用相同供应商的服务器计算机，并使用与将在实际的部署中使用的服务器相同的配置，建立将在全单位内使用终端服务的客户计算机代表。
- 复制本单位的网络配置。如果网络使用以太网和令牌环网两种，必须在测试实验室中也使用两种。若有可能，为实验室建立独立的 Windows 2000 Server 域，这样您可以监视域控制器的性能，而不必考虑网络中其它活动的因素。如果您计划在 WAN 中部署终端服务，设计的实验室时要使用路由器并使用链接模拟器模拟网络延迟时间。
- 如果不同部门使用终端服务器的方法类似但不完全相同，可以在单个测试实验室内大致模拟所有的部门。然而，如果区别很大，必须考虑为每个部门或任务组建立单独的实验室。
- 在测试服务器上部署典型的应用程序组。在确定当用户同时运行不同应用程序时可能出现的任何相互操作性问题时，此步骤是非常重要的。

监视性能

性能监视是测试中以及在终端服务环境中的日常运行的至关重要的组成部分。必须在先导测试阶段的早期建立基线。然后，随着部署的进行，基线可用于与实际性能进行比较。这有助于很快确认系统瓶颈并加以解决。本节将重点介绍分析终端服务性能所要求的主要系统监视器计数器。在这个环境中影响性能的三个主要系统组件是 CPU、内存、和网络。

评估 CPU 性能

检测终端服务服务器中的处理器瓶颈类似于检测 Windows 2000 服务器中的处理器瓶颈，但计数器的基线值可能各不相同。确认瓶颈的最重要的计数器是：

Percent of Total Processor Time (System) / 总处理器时间的百分比（系统）
这是所有系统处理器的活动的度量。在多处理器计算机中，这个计数器等于处理器活动总量除以处理器的数量。在验证了所有的系统处理器都平等地处理线程之后，这个计数器特别有用。

Processor Queue Length (System) / 处理器队列长度（系统） 这是在线程单元中处理器队列的瞬间长度。所有的处理器都使用单个队列，在该队列中各线程等待处理器周期。在处理器可用于在处理器队列中等待的线程之后，线程可以切换到该处理器中执行。处理器一次只能执行一个线程。注意快的 CPU 比慢的 CPU 处理的队列长度长。

Processor Time (Processor) / 处理器时间（处理器） 这是处理器执行非空闲进程的线程的繁忙时间百分比。该计数器为操作系统上每个可用的系统处理器提供一个实例。可以使用它验证每个系统处理器平等地处理等待的线程。

Total Interrupts/Sec / 总中断/秒 计算机接收并服务硬件中断的速率。可能产生中断的一些设备是系统时钟、鼠标、数据通信线路、网卡、以及其它外围设备。可以使用该计数器识别可能占用大量处理器时间的设备驱动程序。

Percent of Total Processor Utilization and Processor Queue Length / 总的处理器使用和处理器队列长度的百分比　这些是识别 CPU 瓶颈系统中瓶颈的最重要的计数器。随着系统处理器越来越忙，在处理器队列中等待执行的线程数量越来越多。

评估内存性能

除了系统监视器计数器，“**任务管理器**”显示物理内存，这在评估终端服务的内存性能时非常有用。可用内存、内存总额、和文件缓存值可以在**任务管理器**内的“**性能**”选项卡中找到。

任务管理器中两个最重要的性能计数器是可用物理内存和页面输入/秒。为防止与内存相关的性能问题，认真观察这些计数器中的减少。减少量是每用户所要求的内存量的很好的指示。作为一个原则，当可用物理内存低于每用户平均内存需求的两倍时，就认为终端服务器内存方面已完全使用。如果观察到页面输入/秒的显著的增加，大概超过了内存容量，那就需要添加另外的内存。

可用字节（内存）在 Zeroed、Free、和 Standby 列表中显示当前虚拟内存的大小。Zeroed 和 Free 内存可供使用，Zeroed 内存被清为零。Standby 内存是从进程的工作区删除的但仍可使用的内存。注意这是瞬间计数，不是时间间隔内的平均值。

页面输入/秒是从磁盘读取的页面数，以解析在调用时不在内存中的页面的内存参照。该计数器包括代表系统缓存访问应用程序的文件数据的分页通信。如果您担心可能产生过度的内存压力和过度的分页，观察此计数器是很重要的。

评估网络性能

即使在 CPU 和内存够用的情况下，由于网络通信的延迟，终端服务性能也可能被认为是无法接受的。

有四个区域可能发生网络通信瓶颈：客户端网络接口、物理网络媒体、服务器客户机到服务器网络接口、或用于服务器到服务器/主机通信的服务器网络接口。网络通信瓶颈直接影响客户工作站上的用户的使用。

跟踪网络使用的最有用的系统监视器计数器是 Network Segment（网段）计数器：

- %Network Utilization（% 网络使用率）是在被监视的网段中正在使用的网络带宽的百分比。
- Total Bytes Received/Sec（接收的字节总数/秒）是网段中每秒接收的字节的总数。
- Total Frames Received/Sec（接收的总帧数/秒）是网段中每秒接收的帧的总数。

使用帮助中心和管理工具

终端服务为帮助中心提供了许多管理工具和远程控制功能，以更好地进行支持工作。

远程控制

远程控制功能允许帮助中心支持专业人员临时控制用户的会话并看到用户的操作。帮助中心还可以与用户交互操作并代表用户执行命令。

为使帮助中心组能够使用远程控制功能，建议在域中创建帮助中心组。在创建组之后，可以使用终端服务配置 MMC 管理单元给组赋予使用远程控制功能的权限。

为利用使用 RDP 的远程控制，两端客户都必须连接到 Windows 2000 终端服务器。

管理工具

当您安装 Windows 2000 终端服务时，有其它一些管理工具被添加到“ 管理工具 ”文件夹。这些工具包括：

终端服务客户端创建器 使用此工具创建在 Windows for Workgroups、Windows 95、Windows 98、和 Windows NT 平台上安装终端服务客户软件的软盘。

终端服务管理器 使用此工具，可以管理所有运行终端服务的 Windows 2000 服务器。管理员可以查看当前用户、服务器和进程。另外，管理员还可以将消息发送到特定用户、使用远程控制功能和终止进程。

终端服务配置 您可用此工具管理 RDP 配置。修改此工具中的选项是全局性的，除非您选择从位于用户配置中的相同选项中继承信息。可用的选项是：设置连接加密、登录设置、超时、成功登录时运行的最初的程序、远程控制选项、Windows 打印机映射、LPT 端口映射、剪贴板映射、和将这些选项应用到特定的 LAN 适配器。

终端服务授权 使用此工具，可以储存和跟踪 Windows 2000 终端服务客户访问许可证。它可以在安装终端服务时或以后安装。当客户登录到终端服务时，终端服务验证客户许可证。如果客户没有许可证或要求更换许可证，终端服务器会从许可证服务器申请一个。许可证服务器从其可用的许可证池提供许可证，终端服务将许可证传递给客户。如果没有可用的许可证，许可证服务器给客户颁发一个临时许可证。在颁发许可证之后，每个客户许可证都与特定的计算机或终端关联。

终端服务部署规划任务列表

表 16.2 总结了在规划终端服务部署时需要进行的工作。

表 16.2 终端服务规划任务摘要

任务	所在章节
选择远程管理或服务器应用程序模式。	终端服务概述
确定授权要求。	终端服务概述
确定如何在业务环境中使用终端服务。	制定终端服务部署规划
记录现有的计算环境。	制定终端服务部署规划
描述部署项目如何满足已明确的要求。	制定终端服务部署设计
制定实现终端服务的规划，包括网络、安全、和域结构。	制定终端服务部署设计
确定服务器部署包括 CPU、存储等的指导方针和标准。	为终端服务部署配置服务器
准备部署到客户机环境。	为客户机部署做准备
准备测试和先导测试部署规划。	测试和先导测试规划

准备提供支持。	使用帮助中心和管理工具

第 17 章 - 确定 Windows 2000 网络安全性策略

现在，大多数单位希望他们的计算机基础结构能连接到 Internet，因为 Internet 能为他们的员工和客户提供有价值的服务。

然而，通过连接 Internet 得到的服务可能会被滥用，这就需要采用网络安全策略。Microsoft® Windows® 2000 包含了许多可在规划网络安全策略时使用的技术。不论网络安全只是本单位内部问题，还是本单位外部连接的是非 Internet 的网络，这些技术都可使用。有关内部安全的详细信息，参见本书的“规划分布式安全”一章。本章将论述如何策略性地使用这些安全技术来保护贵公司与 Internet 或其它公共网络的网络连接。本章没有提供有关如何安装和使用网络安全策略技术的详细信息。从事网络安全设计的网络结构设计师和从事网络安全管理的网络管理员必须阅读这一章。作为执行本章所概述的任务的先决条件，您必须熟悉诸如路由、网络协议和 Web 服务等网络和 Internet 技术。

本章内容

网络安全规划
制定安全网络连接策略
部署网络安全技术
确定网络安全策略规划任务列表

本章目标

本章将帮助您完成如下规划文档：

- 网络安全规划
- 网络安全技术的部署规划

资源工具包中的相关信息

- 有关如何实现和使用 Windows 2000 网络安全技术的详细信息，参见 Microsoft® Windows® 2000 Server Resource Kit Internetworking Guide。
- 有关 IPSec 的详细信息，参见 Microsoft® Windows® 2000 Server Resource Kit TCP/IP Core Networking Guide。

规划网络安全

通过 Internet 连接，本单位的员工可以用电子邮件与世界各地的人们沟通并获得大量不同来源的信息和文件。客户也可以随时从本单位获得信息和服务。另外，本单位的员工可以在家中、饭店或任何可能的地方使用公司的资源，而合作伙伴可以使用特殊设备来更有效地与贵公司合作。

当您规划网络时，要使用适合本单位的安全技术。在 Windows 2000 部署规划早期考虑好这些问题，将确保安全不被破坏，并且在需要的时候能提供安全的网络设施。即使您可能已经拥有安全网络环境，也要切记审查 Windows 2000 功能中的安全策略。考虑 Windows 2000 中新的网络安全技术所产生的影响可以使您重新审视安全规划。建议在制定安全规划的一开始，完成如下任务：

- 评估网络安全风险。
- 确定服务器规模和位置要求。

- 人员准备。
- 制定和发布安全策略和措施。
- 使用正规的方法制定安全技术的部署规划。
- 确定用户组和他们的特殊需求及安全风险。

下面几节将详细论述这些问题。

备注 有关网络部署规划的详细信息，参见本书的“确定网络连接策略”一章。该章讲述了路由、寻址、名称解析、网络应用程序和相关网络问题的策略。本章重点是网络安全问题。

评估网络安全风险

不幸的是，共享和获取信息的能力也会带来巨大的风险。竞争对手可能会试图获取早期的或专有的产品信息，或者有人可能会恶作剧地修改网页或使计算机超负荷而不能工作。也有可能雇员会访问不该访问的信息。必须避免这些或其他安全风险来确保贵公司业务能够按计划进行。为保证只有相关人员可访问资源和数据，仔细审查网络安全技术并合理规划策略是个好主意。通过跟踪网络资源的使用情况，责任也可进一步明确。

有关如何辨别网络安全风险并选择相关策略的一般论述，参见本书的“规划分布式安全”一章。

备注 有些单位不允许连接 Internet 和或任何其它公共网络，以降低网络安全风险。这显然可以限制那些滥用网络设施的那部分人。然而，在单位内仍然存在网络安全风险，并且甚至有限的网络连接也会暴露出一些风险。因此，在这些情况下仍然需要网络安全策略和技术。

图 17.1 是确定网络安全策略的主要步骤。

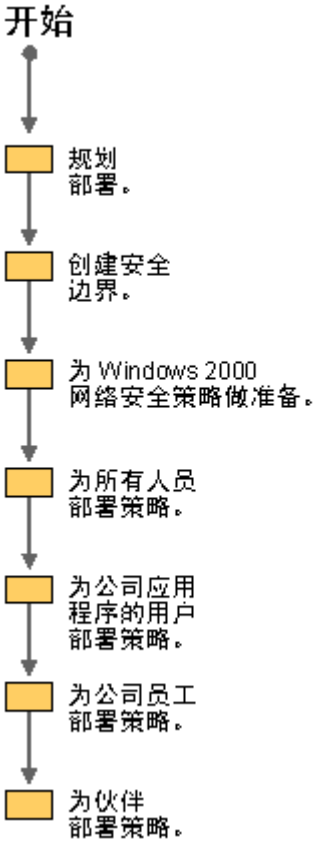


图 17.1 确定网络安全策略的步骤

确定服务器规模和位置

在建立 Intranet 与 Internet 或其它公共网络的连接时，请仔细考虑在何处建立连接。通常应该建立在本单位网络的中心位置，这样服务器和 Internet 间的有效距离大大缩短。服务器位置也应位于网络人员容易到达以便于维护的地方。

最理想的是整个公司与 Internet 只有一个连接。这将简化连接管理并减少由于不一致的策略和措施导致的安全性降低的可能性。

当决定了从何处连接 Internet 之后，必须确定用于支持网络安全技术的服务器硬件。这些服务器的规格取决于您要应用的技术和预计的工作量，但至少它们必须能运行 Windows 2000 Server。尽管在运行网络安全应用程序的相同服务器上运行其它软件程序是可以的，但我们不主张这么做。运行其它应用程序将降低服务器满足网络安全需求的容量，从而可能导致服务器故障。而且，如果应用程序有安全隐患的话，就会危及网络安全。

人员准备

安全技术需要由非常能干和可靠的人员来部署和管理。他们必须将整个网络和网络安全基础结构完美统一，以便消除安全隐患或尽可能减少安全隐患。随着环境和需求的变化，他们必须始终保持网络安全基础结构的完整性。

保证维护网络安全的人员能成功的关键因素是确保他们训练有素并能适应技术更新。他们需要花时间去掌握 Windows 2000，尤其是其网络安全技术。实验和实际应用是这些人员加强培训的必经之路。

另外，网络安全人员必须熟悉网络安全的一般问题。有关这些问题可以从许多书中找到，Internet 也有不少网站论述了网络安全。

制定安全策略和措施

策略和措施通常是重要的，但对于维护安全来说，它们尤为关键。必须建立和发布策略，就如何处理特殊安全问题达成一致，并确保每个人都能清楚地理解这些策略。正规化的措施能确保系统的维护和更改都是经过深思熟虑的。

必须考虑的一个问题是如何监视破坏安全的行为或企图。如果相关的人员能尽早地发现，那么就可以阻止其企图，将破坏减到最小。只有当监视措施到位，这才可能实现。明确的策略有助于建立处理这些安全问题的措施。

可靠性是另一个必须注意的重要的安全问题。必须筹划好某个安全基础结构的组件失效时应急措施。在破坏安全的事件发生前就应决定应采取的行动，并且尽快准备好解决这些问题的资源。

制定部署安全技术规划

使用正规的项目方法，制定部署网络安全技术详细规划，作为总体 Windows 2000 部署规划的一部分。这将确保您能系统地、完整地部署网络安全技术，将失败可能性降到最小。项目的关键步骤包括将网络安全策略传达至所有有关各方，以及将策略和措施传达至网络用户。

部署项目的最重要部分是先导测试。预备采用的网络安全技术需要在一个安全的环境中进行大量和实际的测试。这有助于确保体系结构能按设想正常工作、安全目标能够实现，并确保员工为部署和支持这些技术作好准备。

明确用户分类和他们的安全需求和风险

网络基础结构的建立是基于本单位的切身利益，来为各种人员提供服务的。为了便于本章网络安全策略的讨论，我们把各种人员分成四个网络用户群体。

每个人 这个类别包括任何单位或地方访问网络的所有人，其中可能包含员工、用户和伙伴。他们通常不易准确地识别出，因此必须被看作是匿名的。

员工 这组包括所有为本单位工作的人。使用标准化的内部措施可以很容易地识别他们。他们通常使用公司的电子邮件和 Intranet。

用户 这组包括那些使用应用程序来完成业务工作的人员。

伙伴 这组包括任何单位或地方与本单位有特殊关系的人员。他们遵循标准化程序所以易被识别。他们使用与员工和用户相似的设备。他们经常被当作 Extranet 的一部分。

本章的网络安全策略针对各组网络用户的需求和风险，并详细介绍可以满足他们需求同时使风险降到最低的方法。另外，您还看到安全的总体策略和网络安全基础结构的总体策略。

制定安全网络连接的策略

当您将计算机连接到您还不能完全信任的网络时，网络安全变得尤为重要。单位中的网络安全问题也是很常见的，但针对这些问题，您可以使用很多的责任和纪律，并且也有许多基本的、分布式的网络安全技术来处

理这些问题。在本单位以外，对于责任和纪律的选择大大地降低了，因此必须更多地依赖网络安全技术。

创建安全边界

在本单位和外部世界之间的网络安全取决于您实施网络安全技术的一台或多台服务器。这些服务器逻辑上位于本单位和外部世界之间的边界上。为外部世界提供服务的应用程序服务器通常位于同样的物理位置。

提高这些服务器安全性的一个办法是在逻辑上将它们放置在网络基础结构中的某个独特位置。它们所在的区域通常叫作非军事区（DMZ）。防火墙（将在下一节论述）有一个附加的网络适配器，它依靠分配给 DMZ 区域的一组地址将通信引导到该区域。图 17.2 是这种关系的示意图。

在 DMZ 区域里，可以确保服务器不能访问公司资源。这样的话，即使这些服务器安全被侵犯，作恶者也不能继续进攻 Intranet 里的其它计算机。

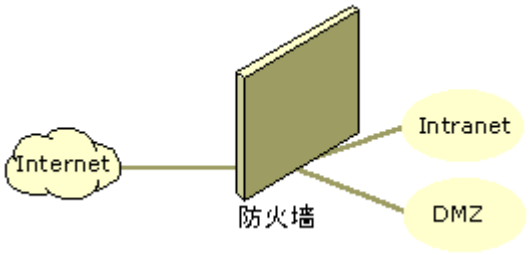


图 17.2 非军事区

DMZ 与所有内部网络组件一样，需要对它们进行物理保护，以防止外界访问。这将确保没有任何人 — 甚至雇员也不能够通过重新布线或使用登录帐户来降低安全性。

您不必在物理上将 DMZ 与其它计算机和网络设备分开。然而，由于其在网络安全中的重要地位，将一些特殊的策略和措施应用到 DMZ 中是恰当的做法。哪怕是极小的不当的改动，也能足以产生入侵者可以利用的安全疏漏。因此，决不允许无资格人员改动 DMZ。对 DMZ 采取更严格的物理安全保护能确保这种安全。

注意 精心保障您计算机和帐户的安全，以确保只有经授权的用户可以使用它们访问网络。如果您不能用物理方式保障客户机的安全，那么一定要保证在上面使用的帐户没有优先权限，并且使用文件加密、安全的屏幕保护程序和其它本地安全策略。

提防任何人

为保障本单位网络与 Internet 之间访问的安全，必须在两者之间加入一个服务器。此服务器为公司员工提供与 Internet 的连接而又能使由此连接带来的风险降到最小。同时它还阻止从 Internet 到公司网络的计算机的访问，但那些经授权具有访问权限的计算机例外。

这个服务器运行防火墙或代理服务器软件。它有两个网络接口：一个用于公司网络而另一个用于 Internet。防火墙或代理服务器软件检查每个接口的所有网络数据包，以确定它们的发送地址。如果通过软件标准的检查，这些数据包将在合适的地方传递到其它接口以分发到相应网络的其余部分。

在某些情况下，数据包内容传递时显示的是来自代理服务器，但当结果返回到代理服务器时，会被传递到请求计算机。这能确保在 Internet 上的人不能获取代理服务器以外的计算机地址。

使用 Microsoft Proxy Server

Microsoft® Proxy Server 2.0 同时具有代理服务器和防火墙功能。Proxy Server 2.0 在 Windows 2000 运行，

两者都需要进行合理的配置，以便获得全面的网络安全。如果您的 Proxy Server 比带 Service Pack 1 的 2.0 版更早，必须在将服务器升级至 Windows 2000 的时候，将这个版本升级以便与 Windows 2000 兼容。

在许多情况下，公司网络与 Internet 之间的通信量超过了一台代理服务器能够处理的通信量。这时，可以使用多台代理服务器；通信自动在它们之间协调。对于 Internet 和 Intranet 两端的用户，就好象一台代理服务器工作一样。

要使用高级的 Microsoft Proxy Server 功能，计算机需要安装 Microsoft Proxy Server 客户和配置以便能够使用代理服务器。没有客户的计算机（如那些 Internet 上的）作为匿名用户，从代理服务器获得基本的服务。

在连接 Internet 之前，一定要测试代理服务器。建立一个小规模 Internet 和 Intranet 的模型，让客户机尝试从两个方向访问不同的服务。并且尝试未经授权的连接来验证网络是否拒绝。确保测试大量不同类型的网络访问方法来验证所有类型的网络访问是安全的。尝试能利用安全漏洞的各种不同技术，以保障环境里没有这样的漏洞。有关网络安全的书籍提供了测试特殊问题的建议。第三方产品和在此领域有丰富经验的咨询公司也有助于这样的测试。

这些产品包含了使用 Microsoft Proxy Server 的步骤。有关 Microsoft Proxy Server 的更多信息和 Microsoft 安全技术的详细资料，参见 Web 资源页的 Microsoft Security Advisor 链接，网址是 http://windows.microsoft.com/windows2000/reskit/webresources。

监视网络安全

只有当您仔细地计划和配置，您所实现的网络安全技术才能达到预定目标。只要准备充分，此项工作可以胜利地完成。然而，对所有风险作预测是非常困难的，因为新的风险不断在酝酿，系统故障以及您系统所处的环境不断地在变化。即时地审查网络安全策略可以使这些风险降到最低。但是，还需要监视网络安全的真实活动，在安全隐患爆发前能找出它们，并在破坏安全的企图得逞前阻止它们。

要监视网络安全活动，需要一些工具来捕获这些活动详细信息和分析这些数据。Microsoft Proxy Server 包含两个级别的日志：正常和详细。Windows 2000 也有事件日志，它可以通过启用安全审核来得到加强。将在本章稍后论述的 Internet 验证服务器，具有扩展的活动报告选项。第三方产品也有助于监视服务器和应用程序，包括安全服务器和应用程序。无论使用何种计算机，一定要仔细阅读文档并且选择最能满足需要的日志选项。

连接外部网络

当代理服务器到位，并具备了监视设施和合理安排的人员，便可以连接网络到外部网络。进行最后一轮的测试以保证部署按计划顺利完成。要确信只有您授权的服务可用，而滥用的风险几乎不存在。此环境需要细心监视和维护，但您也要准备考虑提供其它网络安全服务。

备注 本章不讨论如何建立网络连接。有许多书籍包含了这个主题，网络服务提供商能建立这种连接、或者会提供能建立这种连接的咨询公司的联络信息。

部署网络安全技术

当准备好总体网络安全策略后，可以决定如何对本章定义的每个用户群体使用增强的网络安全技术：“ 每个人 ”、“ 员工 ”、“ 用户 ”和“ 伙伴 ”。然后可以为每个网络用户群体部署网络安全策略。可先将“ 每个人 ”看作一组，考虑其需求，然后将公司“ 员工 ”、公司应用程序的“ 用户 ”以及“ 伙伴 ”作为业务优先指令组考虑。

在确定本单位的特殊安全策略之前，必须考虑增强网络安全的 Windows 2000 的功能。

为 Windows 2000 网络安全技术做准备

在某些情况下，Windows 2000 网络安全技术取决于其它 Windows 2000 安全技术。比如，虚拟专用网络的“第二层隧道协议（L2TP）” 使用 IPSec 来提供从远程客户到 VPN 服务器的安全。IPSec 安全协商需要证书来授权连接。因此，要有一个合理配置的证书服务器。通常在域中加入一个 Windows 2000 证书服务器。此域用公钥基础结构（PKI）设置来指定“组策略”，使计算机能在这个证书颁发机构自动登记，并得到 IPSec 的计算机证书。L2TP 创建必要的 IPSec 策略来保证 L2TP 通信是安全的。但是，管理员可能也想保证所有服务器和客户机之间的其它通信的安全。这需要在每台服务器和客户机上配置 IPSec。因为 IPSec 是用某个策略来配置的，当您在 Active Directory™ 目录中建立了这个策略以后，可以在一个组或域的基础上将它应用到所有计算机上。可以通过使用 Active Directory 目录中“组策略”的集中管理，来将证书和 IPSec 策略部署至所有域计算机。

有关规划部署 Windows 2000 证书的详细信息，参见本书中的“规划公钥基础结构”。有关 Active Directory 规划的详细信息，参见本书的“设计 Active Directory 结构”一章。

为“每个人”部署策略

当 Internet 连接就位，任何能找到此连接的人都会带来潜在的网络安全风险。因此，当您部署总体网络安全策略时所要面对的第一用户群体，就是前面定义的“每个人”。通过设置代理服务器及安全监视策略、措施和技术，可以部分地完成这个工作。

或许您也想考虑“每个人”从中受益的网络应用程序和这些应用程序的安全要求。比如，您可能想在内部 Web 站点建立 Microsoft Internet 信息服务 (IIS)。IIS 有许多安全选项需要您仔细考虑和配置。（IIS 包含有关这个主题的扩展文档。）也可考虑使用文件传输协议（FTP）服务器和“每个人”能从中受益的其它服务。

为“员工”部署策略

“员工”组里的人可能想从任何位置访问其公司网络，以便访问内部 Web 站点、复制文件、打印文档以及其他简单功能。在这种情况下，主要安全目标是在“用户”访问网络前，先验证“用户”是经授权的雇员。因此，与网络的初始连接必须是安全的，但不需要进一步确认。需要进一步关注的是必须阻止未经授权的人中途截取和读取网络上的通信。

雇员可以使用 Internet 服务提供商（ISP）来访问公司网络；并不是所有员工具有这种访问权。您可能不想通过 Internet 提供所有 Intranet 服务，或者想保障专用网络链接有一定的网络容量。使用“Windows 2000 路由和远程访问”服务，可以非常具体地定义远程访问策略，比如用户如何在连接 Internet 时访问内部网络。

路由和远程访问

各单位通常在它们自己的站点上为员工提供远程连接选项。IT 人员为此建立专用的电话号码，并且将调制解调器（或类似硬件）连接到一个直接连接 Intranet 的服务器上。此服务器能运行特殊的软件来处理连接的详细信息，而且它也能将拨号用户当作一个经授权的员工进行身份验证。

Windows 2000 的路由和远程访问使您能够为用户提供拨号设备。如果您想在 Windows 2000 中集中管理用户身份验证、授权、和计帐服务，可以通过安装一个 Internet 验证服务 (IAS) 服务器来使用远程访问或 VPN。图 17.3 是这些服务器的一种可能的配置示意图。

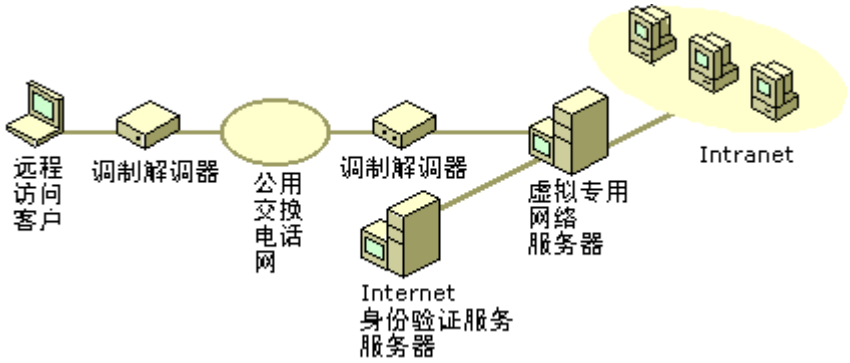


图 17.3 路由和远程访问配置示例

Microsoft® Windows® 2000 Server Resource Kit Internetworking Guide 中包含有关路由和远程访问工作原理及其功能信息。Windows 2000 Server“帮助”描述了如何安装和使用路由和远程访问。

规划部署路由和远程访问时，请考虑以下安全问题：

- 谁将拥有电话号码？
- 谁将拥有使用路由和远程访问的权限？
- 将使用哪一种身份验证方法？
- 如何使用数据加密（从路由和远程访问客户到路由和远程访问服务器）？

  如果需要端对端加密（从远程访问客户一直到内部网络上的应用程序服务器），使用 Internet 协议安全（IPSec），该协议安全在本章稍后讨论。

- 将使用哪些远程访问策略对用户访问进行控制？

有关路由和远程访问的一般部署问题的详细信息，参见本书中的“确定网络连接策略”。

路由和远程访问安全

限制路由和远程访问电话号码的分配有助于最大限度地减少试图拨号入网的人数。但是由于任何人都有可能获得电话号码，因此任何一种拨号连接解决方案仍会存在风险。可以设立一套按次序拨打电话号码的自动过程，直到查找到应答的调制解调器为止。因此，路由和远程访问需要有安全措施以保证只有经授权才能访问。路由和远程访问至少应要求用户提供有效的计算机帐户及密码。但是此安全等级很容易受到各种通常的登录攻击，如猜测密码。

建议使用额外的路由和远程访问安全选项。可限制路由和远程访问的使用，只允许拥有经确认的业务需求的人员拨号进入。也可要求路由和远程访问先挂断初次建立的连接然后再往回拨打给用户。通过这种方式，用户只能从某一预先确定的电话号码对路由和远程访问设备进行访问，或可以把电话号码记录下来。在设备允许的情况下，也可使用呼叫方 ID 记录下呼叫端的电话号码。

应考虑到当用户尝试登录到路由和远程访问服务器时，某人会使用类似于窃听装置的技术拦截用户名和密码。要防止这类事件的发生，路由和远程访问可使用一种安全的用户身份验证方法，例如可扩展身份验证协议（EAP）、Microsoft 质询握手身份验证协议（MS-CHAP）第一版和第二版或 Shiva 握手身份验证协议（SPAP）。

与此相关的风险是用户相信他或她正在拨入公司网络，但实际上拨入的是正在获取有关他们身份信息的另一

站点。要避免这类事件的发生，可使用相互身份验证以确保路由和远程访问服务器是经过授权的，如同用户经授权一样。这一方法对 EAP 传输层安全（EAP-TLS）或 MS-CHAP 第二版身份验证协议都是可行的。

对于在路由和远程访问连接上进行传送的数据也存在着类似的问题。EAP-TLS 或 MS-CHAP 第二版身份验证协议允许您在数据传输的同时使用 Microsoft 点对点加密（MPPE）对数据加密。

远程访问策略，无论是作为本地策略还是组策略的一部分实施，可加强您所选择的身份验证以及加密技术的使用。

关于网络、路由和远程访问身份验证以及数据加密技术的详细信息，参见 Windows 2000 Server“帮助”。

虚拟专用网络

虚拟专用网络（VPNs）在公共网络上提供安全的网络服务，类似于专用网络，但成本更低。VPN 允许公司员工和其他经授权用户从远端位置连接到企业网络，并与从公司站点连接一样安全。因此，所有的企业网络服务都可通过 VPN 安全地提供。VPN 比不安全的公用网络连接需要投入更多的精力进行学习、安装和支持。但是 VPN 使用低成本的 Internet 或类似的连接方式提供全面安全的连接。

可以与路由和远程访问一起使用 VPN，但并不要求。可使用任何一种链接方式在站点之间建立 VPN，而且也可在某个站点内使用以加强安全。

虚拟专用网络的典型工作方式如下：

- 用户拨入 Internet 服务提供商（ISP）。
- VPN 客户软件通过 Internet 与贵公司的指定的 VPN 服务器联系，并启动身份验证。
- 对用户进行身份验证并提供安全详细信息。
- VPN 服务器向客户计算机提供一个新的传输控制协议/Internet 协议（TCP/IP）地址，然后客户计算机接受指令使用新的地址通过 VPN 服务器发送所有其它的网络通信。
- 之后，所有的网络数据包在交换过程中被全部加密，只有 VPN 客户和 VPN 服务器可以解密。

图 17.4 是这些计算机之间的关系示意图。

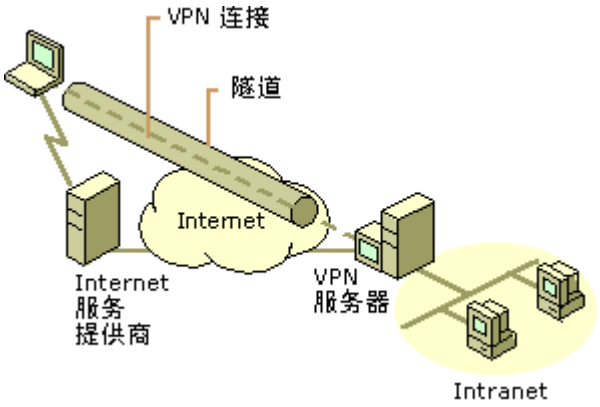


图 17.4 虚拟专用网络配置示例

也可使用 VPN 将某一站点的多个计算机连接到企业网络，或者用一子网限制通信，只允许经授权人员使用。

Windows 2000 Server 包括 Windows 2000 VPN 软件作为路由和远程访问的一部分，是Windows 2000 组件的可选组件。Internetworking Guide 包含有关 Windows 2000 VPN 的工作原理及其提供设备的详细信息。Windows 2000 Server“帮助”详述了如何安装 VPN 的信息。

部署 VPN

如果您计划部署 VPN，需要考虑不同的问题，例如：

- 要使用哪个安全协议 —— 点对点隧道协议 (PPTP) 还是第二层隧道协议 (L2TP)。
- 是否使用 IPSec （如果选择 L2TP）。
- 以 L2TP/IPSec 连接时使用什么证书。
- 将 VPN 服务器置于何处 — 在防火墙前面、后面还是旁边。
- 如何使用连接管理器给予用户预先确定的设置。
- 如何使用 VPN 作为远程访问策略的一部分。

PPTP 与 L2TP

点对点隧道协议 (PPTP) 是一种 TCP/IP 网络协议，内含了 IP、IPX 或 NetBIOS 增强型用户接口 (NetBEUI) 协议。PPTP 允许 Internet（或类似网络）上的非 TCP/IP 或多协议网络活动。基于 PPTP 的 VPN 也提供用户身份验证、访问控制并应用拨号配置文件，以便仔细限制某些远程访问类型使其只能由特定用户使用。PPTP 为远程客户提供内部地址配置，使他们能参与内部网，好象直接连网一样。PPTP 针对隧道中传输的通信提供标准和加强 RC4 （对称流密码）加密压缩和选项。

L2TP 与 PPTP 非常相似，但是使用 UDP，因此可在异步传输模式 (ATM)、帧中继以及 X.25 网络上使用。L2TP 在 IP 网络上使用时，在控制信道和数据信道上使用 UDP 端口 1701 数据包格式。L2TP 也可与 IPSec 一同使用，提供全面安全的网络链接。IPSec 在客户和 VPN 服务器之间进行 L2TP 通信时，首先进行安全协商，使用证书进行身份验证。然后，L2TP 使用用户帐户和密码或使用用户证书提供身份验证。

Internet 协议安全

Internet 协议安全 (IPSec) 是保证 Internet 协议 (IP) 网络通信安全的协议。IPSec 提供两台电脑间的绝对安全，因此任何部分都是安全的。使用 IPSec 策略对 IPSec 进行配置。这些策略可包含多项安全规则，每项规则详细说明过滤器的通信特定类型，与过滤器操作和身份验证方法有关。IPSec 策略可在本地计算机或组策略中的 Active Directory 内创建或指派。

备注 IPSec 确实提供端到端的 IP 安全，但不对 IP 上运行的所有协议加密。IPSec 对某些特定的通信具有内置免加密作用，例如 Internet 密钥交换协商、Kerberos 身份验证、IP 广播以及 IP 多播通信。如需要，可通过创建 IPSec 规则对额外协议进行免除，使用过滤器指定通信类型和许可的过滤器操作。

关于 IPSec 的详细信息，参见 Windows 2000 Server“帮助”和 TCP/IP Core Networking Guide。有关在公钥基础结构中规划部署证书颁发机构的详细信息，参见本书中的“规划公钥基础结构”。

VPN 服务器位置

可与防火墙一起使用 VPN。虽然 VPN 的作用与防火墙类似，无论是防火墙还是 VPN 都能提供对方没有的其他优点，因此二者可能都需要。在这种情况下，应考虑 VPN 服务器与防火墙相对位置。

物理上，可将二者安装在同一台服务器上。这样一来，如果服务器不能用或是服务器的安全被损坏，两者就

会同时出故障。但是，服务器数量越少，服务器的不可用性也就越小，同时降低了服务器的维护成本。还有与容量有关的问题。应考虑每个因素如何影响确定您所需要的特定设计的情况。

更为重要的问题是 VPN 服务器与防火墙的逻辑关系。如图 17.5 所示的选项，从逻辑上讲，VPN 服务器将在放火墙前面、后面或旁边。Windows 2000 可提供防火墙服务，要么使用 Proxy Server，要么使用数据包过滤器路由。有关各种解决方案的详细信息，参见 *Internetworking Guide* 中的“Routing and Remote Access Service”。

VPN 服务器位于防火墙前面时，防火墙只向经授权的 VPN 用户提供外部服务。因此，不提供一般的 Internet 访问或类似访问。VPN 连接的远端提供 Internet 访问时例外。

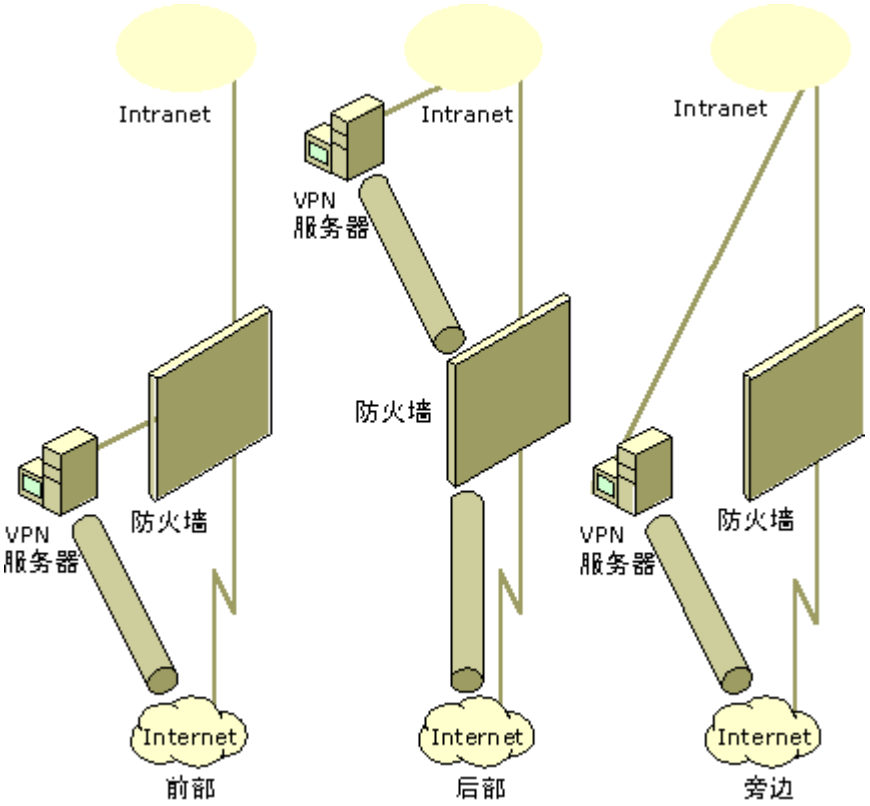


图 17.5 VPN 服务器相对于防火墙的逻辑位置示例

VPN 服务器位于防火墙后面时，防火墙提供所有传统服务，但需要将其配置打开 VPN 服务器所需要的端口。如果与 IPSec VPN 一起使用 L2TP，上述配置应包括 IPSec 所需的端口。

VPN 服务器位于防火墙旁边时，VPN 服务器或防火墙各自独立地提供服务。但是，这种配置为企业网络提供了两个访问路由，增加了安全被破坏的潜在危险。通常，VPN 服务器或防火墙都不在对方附近提供路由，但是既然有两个路由，风险也就增加了一倍。

如何选择适合您自身情况的最佳关系取决于您感到最为得心应手的安全措施。由于两个服务器相互比邻，两个路由接入到 Intranet 中，因此也就存在着两个安全风险。若 VPN 服务器在防火墙后面，就必须在防火墙上打开更多的端口。若 VPN 服务器在防火墙前面，VPN 服务器不会从防火墙所提供的安全中受益，但是它处理的所有通信量的确能从防火墙受益。

连接管理器

向用户提供 VPN 设备需要在每台客户计算机上进行一些配置。设置起来并不一定简单，但是 Windows 2000

包括一个连接管理器，使用户设置过程更为简便。

连接管理器可在运行 Microsoft® Windows 95®、 Microsoft® Windows® 98、 Microsoft® Windows® NT 或 Windows 2000 的计算机上运行。Windows 2000 服务器也有一套管理工具包，名为“ 连接管理器管理工具包 ”，可使您为用户创建自定义连接管理器。

有关连接、连接管理器以及连接管理器管理工具包的详细信息，参见 Windows 2000 Server “ 帮助 ”。按照 Windows 2000 Server“ 帮助 ”中的说明进行操作并运行连接管理器管理工具包后，您会有一程序及文档分发给用户。

远程访问策略

远程访问策略允许您指定可以使用路由和远程访问的人员，以及他们在连接时要应用的不同条件。可基于用户所在的 Windows 2000 组、他们所使用的电话号码、当日时间以及其他相关信息指定策略。策略可规定是否接受或拒绝连接以及可将配置文件应用到连接上。配置文件可规定会话持续时长、空闲时长、允许使用哪种拨号媒体、允许使用哪些地址、需要哪些身份验证方法以及需要加密还是 VPN。

可对路由和远程访问或 Internet 验证服务 (IAS) 设置远程访问策略，本章稍后将对此进行讨论。有关远程访问策略，包括如何进行设置以及策略提供的选项的详细信息，参见 Windows 2000 Server“ 帮助 ”。

应认真考虑针对不同的组或不同的情况使用不同的策略。策略可以相互重叠从而使您本来允许拨号上网的人员受阻或是导致其他问题。复杂的策略组合使这些问题更容易发生。因此，最好的方式是尽可能地使策略数量缩减到最小。Windows 2000 Server“ 帮助 ”包括一旦出现问题如何排除远程访问策略故障的推荐步骤。

VPN 服务器容量

和所有的服务器一样，如果 VPN 服务器处理过量的活动，会被工作压垮。必须多个 VPN 链接以应付这类事件的发生，但是对规模较大的单位来讲会是个问题。在先导测试中，可测试用户有可能将多大的信息量加载到所有可用的 VPN 服务器上。也可估计在同一时间可能有的用户量及他们有可能传送的数据量，来测试 VPN 服务器的容量大小。然后可使用局域网络 (LAN) 上的少量客户计算机，并使用大量的活动如复制大量的文件通过 VPN 传送一定数量的数据进行比较。通过监视 VPN 服务器及其响应能力，可确定 VPN 服务器是否有能力担此重任。如果需要，您可增加服务器的大小，或添加更多的 VPN 服务器，使用网络负载平衡服务或循环 DNS 以平衡负载。

Internet 身份验证服务

Windows 2000 Server 包含有 Internet 验证服务 (IAS) 作为可选组件。该服务执行符合工业标准的网络身份验证安全协议，即远程身份验证拨入用户服务 (RADIUS)，允许帐户授权集中化。RADIUS 还允许您指定会话的时间长短以及可使用的 IP 地址。IAS 也可记录会话的详细资料，提供说明和报告选项。

如果您想将远程访问设备外包给他人，但又能对试图使用那些设备的人员的身份验证进行控制，也可使用 IAS。在这种情况下，承包商可将从路由和远程访问服务器的授权请求转至 IAS 服务器。IAS 依据原始的 Windows 2000 域和 Windows NT 4.0 域对帐户进行身份验证。

需要将 IAS 服务器置于防火墙后面，打开服务器上的端口以便进行 RADIUS 身份验证和适当的用户数据报协议 (UDP) 数据包传送。

有关安装和使用 IAS，包括操作建议的详细信息，参见 Windows 2000 Server“ 帮助 ”。Windows 2000 Server “ 帮助 ”中还包含其他安全措施的最佳做法以及在大的环境中对 IAS 进行缩放和有效使用 IAS 日志记录的详细信息。

为用户部署策略

有些用户可能希望当他们不在办公室的时候能对安全的公司应用程序进行访问。有些应用程序比较简单，比如时间管理、公司福利登记或类似的程序。其他应用程序相对复杂，比如计帐系统和业务线应用程序。确保这些应用程序的安全，以便只有经过授权的用户才能对数据进行访问并只能经过授权才能更改。应用程序的使用情况可以跟踪到特定的用户，因此也可明确责任。

Windows 2000 包含多种不同的安全技术，为应用程序开发人员提供了包括网络安全的选项。这些技术的选择取决于：

- 应用程序的安全需求
- 集成问题
- 开发人员对技术的熟悉程度
- 网络和应用程序的性能影响
- 管理复杂性

面向应用程序的网络安全技术包括：

- 安全支持提供商接口（SSPI）— 可从标准的编程接口提供访问多种安全服务的一般安全 API。
- Windows NTLM 安全，也称之为 Windows NT 域级安全。
- **Kerberos v5 身份验证协议**有关的详细信息，参见本书的“规划分布式安全”一章。
- 安全套接字层 (SSL)SSL 已被 Internet 工程任务组（IETF）增强并标准化为传输层安全（TLS)。
- 证书，本章前面部分曾对此进行讨论。

这些网络安全技术以及访问它们的网络技术彼此相互关联，其关系如图 17.6 所示。注意图中的 SSP 代表 SSPI 安全提供商，表示安全设备和 SSPI 之间的接口。.远程过程调用（RPC），Microsoft® 分布式组件对象模型（DCOM),以及 Windows 套接字（Winsock）都属于进程对进程的通讯方法。WinInet（Windows Internet API）是一种用来启动和管理 Web 接口的编程接口。

网络安全技术位于图中的下半部分，从 SSPI 开始。网络技术在图中的上半部分，位于使用网络技术的应用程序框下方。

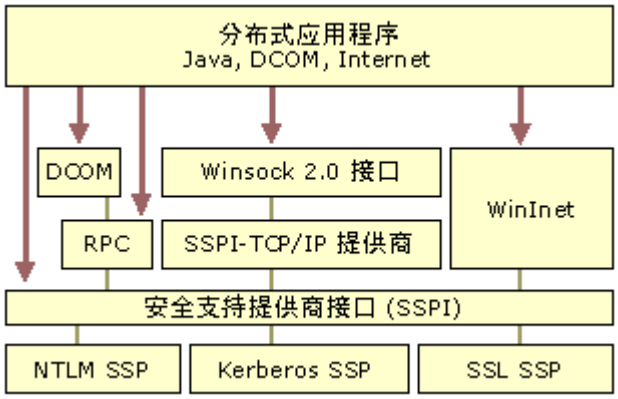


图 17.6 网络应用程序安全技术示例关系图

与您企业的应用程序开发人员及供货商合作，决定必须部署的面向应用程序的安全技术。这些技术不需要更多的基础结构规划，但是必须确定开发人员如何从 Windows 2000 提供的更强大的网络安全中受益。例如，他们会考虑在安装路由和远程访问或 VPN 链接时使用智能卡以保证安全的用户身份验证。

为伙伴部署策略

大多数单位处在复杂的关系网中，包括与客户、供货商、联盟公司、供应商、咨询公司、上级管理部门以及其他与该单位打交道的部门之间的关系。多数伙伴，正如他们的称呼一样，可直接访问贵公司的数据和应用程序，并从中大大受益。但是，提供这种访问路径可能会存在很大风险，将有用的或敏感的信息透露给不应透露的人，或是使某些人恶意控制企业的计算机基础结构。因此，必须有效采用网络安全策略，以便只向伙伴提供最适当的访问。

允许伙伴访问企业网络的网络和安全技术集合通常被称为 Extranet。Extranet 经常使用上文中讨论过的相同技术向员工和用户提供访问权限，例如 VPN 以及路由和远程访问。伙伴的一个明显特征是，他们可经常从某个特定的地点或通过某一预先确定的链接与公司进行通信。因此，您可对代理服务器进行配置，只允许来自该网络地址的 Extranet 链接进入。

在考虑哪些伙伴可使用 Extranet 时，一定要确定他们将与那些业务部门进行通讯交流。一般来讲，伙伴属于那些主要与公司的特定部门进行通讯的不同类别。有些会与收发货物部打交道，其他的会与工程部或销售部进行合作。

为伙伴部署网络安全策略与为用户或员工部署网络策略不一样，主要原因是 Extranet 能迅速成为合作伙伴的任务关键。企业员工通常可以选择进入办公室获取企业资源。而伙伴只能选择使用 Extranet（或采用传统方式）。员工也可能会在某个给定时间使用相对少量的数据，而合作伙伴经常会产生大量数据，需要由计算机进行处理或通过网络进行传送。

合作伙伴与业务部门也对 Extranet 服务的及时性非常敏感。业务活动通常以来交换的数据，延误的代价会相当高。Extranet 应该可靠，而且出现问题时，合作伙伴与业务部门应能与可快速解决问题的人员取得联系。

通过 Extranet 提供服务的业务部门应考虑特殊的问题和限制。在与公司的其他部门进行比较时，系统和员工的经历也有所不同。因此，有些业务部门的 Extranet 需求与其他业务部门不同也是正常的。

出于这些原因，为伙伴部署网络安全的策略需要强调可靠性、可扩展性、灵活性和可支持性。人员安排尤其重要，全面的先导测试、制定策略和措施以及通讯都很重要。包含于 Windows 2000 的网络安全技术为安全的 Extranet 打下基础，但是 Extranet 安全策略和 Intranet 之间的主要区别在于策略和措施。

确定网络安全策略规划任务列表

表 17.1 摘要列出了规划网络安全时必须执行的任务。

表 17.1 确定网络安全规划任务列表

任务	章节中的位置
规划部署。	规划网络安全
创建安全边界。	创建安全边界
为 Windows 2000 网络安全技术做准备。	部署网络安全技术
为每个人部署策略。	为 Windows 2000 网络安全技术做准备
为公司员工部署策略。	为 Windows 2000 网络安全技术做准备
为公司应用程序的用户部署策略。	为用户部署策略
为伙伴部署策略。	为伙伴部署策略

第 18 章 - 确保应用程序和服务的可用性

如果您不能承担由于执行关键任务的应用程序或服务出现中断而造成生产效率下降的损失，或者您的单位要为应用程序或服务承担法律信用责任，本章对您来说，将是很重要的规划章节。

尤其是，本章会帮助系统管理员确定系统是否需要群集，如果需要，又是哪种群集技术最适合本单位的应用程序和服务。本章提供的指导方针将帮助您制定规划，使关键任务应用程序和服务在任何环境下对用户都有高可用性。

本章内容

本章目标

本章将帮助您创建以下规划文档：

- 群集部署规划工作表

资源工具包中的相关信息

- 有关 Microsoft® Windows® 群集的更多信息，请参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide* 中的“Windows Clustering”。
- 有关制定测试规划的更多信息，请参见本书的“建立 Windows 2000 测试实验室”。

提高应用程序和服务的可用性

在任何单位中，服务器故障都会带来极大的损失，不论是文件服务器、打印服务器、Web 服务器、还是应用程序服务器。要精确计算服务器、应用程序或服务停工带来的损失可能相当困难。潜在的损失可能包括：

- 销售额损失
- 顾客信誉损失
- 员工效率和信心的丧失
- 修复带来的费用增加
- 不能履行合同义务及可能引发的法律责任
- 易腐烂产品造成的浪费

- 竞争力的丧失

执行关键任务的应用程序或服务中断，自然会增加单位的损失。如果不能让关键任务应用程序和服务对用户有高可用性，您必将承担高价的风险。

本章讨论了 Windows 群集部署规划的细节问题。群集是 Windows 2000 Advanced Server 的一个功能；对网络和系统管理员来说，它有四个主要优点：

- 应用程序和服务的高可用性。
- 特定应用程序和服务的可扩展性（当使用负载平衡时）。
- 集中的管理。
- 滚动式升级（分别升级群集各节点，而同时让其它节点继续提供服务的过程）。

Windows 2000 Advanced Server 概述

Windows 2000 Server 家族目前包括 Windows 2000 Server 和 Windows 2000 Advanced Server。Windows 2000 Server 为那些拥有众多工作组和分支机构及需要文件、打印、通信、基础结构和 Web 等基本服务的中小型单位提供了适合他们的核心功能。Windows 2000 Advanced Server 的设计是为了满足对关键任务的要求，比如大型数据仓库、联机事务处理 (OLTP)、通信、电子商务或大中型单位及 Internet 服务提供商 (ISP) 需要的 Web 主机服务。

Windows 2000 Advanced Server 从 Microsoft® Windows NT® Server 4.0 企业版发展而来。它提供了全面的群集基础结构，使应用程序和服务的可用性和可扩展性大大提高，其中包括，在 Intel 页面地址扩展 (PAE) 系统中支持高达 8 GB 的主内存。Advanced Server 专为高要求的企业应用程序设计，因而支持使用多达 8 路对称多处理 (SMP) 的新系统。SMP 允许计算机系统的多个处理器同时运行操作系统或应用程序线程。Windows Advanced Server 非常适合数据库密集型的工作，同时它提供了具备高可用性的服务器群集和负载平衡，从而可以提高系统和应用程序的可用性。

Windows 2000 Advanced Server 包括 Windows 2000 Server 的全部功能，并加入了针对企业和大型部门解决方案的高可用性和可扩展性。Advanced Server 的主要功能包括：

- 网络 (TCP/IP) 负载平衡
- 基于 Windows NT Server 4.0 企业版 Microsoft Windows 群集服务 (MSCS) 的增强双节点服务器群集
- Intel PAE 系统中高达 8 GB 的主内存支持
- 多达八路 SMP

备注 如果您不能确定是否有 Intel PAE 计算机系统，请与硬件供应商联系核实。

提高应用程序和服务可用性的过程

规划部署 Windows 群集时，考虑有助于避免服务器、应用程序或服务发生故障的解决方案至关重要。在您规划本单位的应用程序和服务的高可用性时，不妨考虑使用图 18.1 流程图所示的过程。

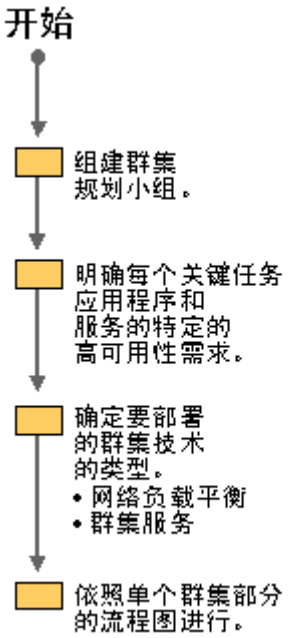


图 18.1 规划应用程序和服务的可用性

在规划阶段开始之前，很重要一点是彻底弄清那些能让关键任务应用程序和服务对单位中的最终用户有高可用性的主要 Windows 群集组件。

Windows 群集概述

“群集”是一组独立的计算机，它们一起运行一组应用程序或服务，并为客户和应用程序提供单一系统映像。群集计算机在物理上用电缆连接，而在程序上通过群集软件连接。这些连接让计算机能够使用“问题求解型”功能，比如负载平衡和故障转移，而这在独立的计算机上是不可用的。

“负载平衡”将服务器负载分配到所有配置的服务器，并防止一台服务器超负荷工作。反过来，这让您可以逐步地扩充容量以满足需要。“故障转移”可以自动将资源从发生故障或脱机的群集服务器转移到工作正常的服务器，从而为用户提供持续的支持。这使群集用户可以不间断地访问资源。目前，Windows 群集提供了以下两项群集技术：

网络负载平衡　网络负载平衡将多达 32 台运行 Windows 2000 Advanced Server 的服务器并为单一负载平衡群集，从而使基于 TCP/IP 的应用程序和服务的可扩展性和可用性大大提高。最常见的网络负载平衡应用是，将入站 Web 请求在 Internet 服务器应用程序（如 Internet 信息服务应用程序）群集间分配。

群集服务　使用 Advanced Server，群集服务让你可以将两台服务器并为一个服务器群集，从而确保关键任务应用程序和资源保持对客户可用。服务器群集让用户和管理员可以在访问特定资源时，把服务器（或节点）看作单一的系统而不是分立的计算机。

在规划和部署高可用性的应用程序和服务时，确定适合本单位的最佳做法至关重要。Microsoft 开发了一系列这方面的最佳做法指南。有关这些指南的更多信息，请参见 Web 资源页的“Microsoft TechNet High Availability”链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

确定可用性策略

在了解了 Windows 群集的功能之后，您便可以开始群集部署的规划阶段，让关键应用程序和服务对单位的用户有高可用性。

组建群集规划小组

在确定群集要求时，协作是至关重要的。对群集策略的规划必须是一个合作项目，要涉及网络管理员和以下应用程序和服务的管理员：

- Microsoft® SQL Server™ 或其它数据库
- Microsoft® Exchange Server 或其它群件
- Microsoft® Internet 信息服务 (IIS) 或其它 Web 服务
- Windows 2000 终端服务
- Windows Internet 命名服务 (WINS)
- 动态主机配置协议 (DHCP)
- 内部开发的业务流程应用程序
- 第三方应用程序
- 文件和打印共享

大多数单位中，这些应用程序和服务都要求对用户有高可用性。

群集规划核心小组必须明确提到的每项关键任务应用程序和服务对高可用性的特定需求。这个小组的全体人员必须都充分了解这些应用程序和服务的用途，以及网络的用途，以避免潜在的高代价的错误。

在确定了群集策略之后，请安排与群集规划核心小组开会，以确定在单位中进行群集配置的人员要求。运行于群集的资源和应用程序与运行于独立服务器上的相同资源会要求不同的管理方法。因此要保证您已经明确了这些区别，并相应地进行了人员培训。同时，要确信这些人员已经明确了对高可用性的要求，明白他们的行为会限制或降低系统的可用性。例如，如果管理员在向包含几百个其它资源的组中添加新资源时配置不当，就可能使整个组（及所包含的资源）的性能降低。

明确应用程序和服务的高可用性要求

要明确单位对关键任务应用程序和服务高可用性的要求，请确定以下事项：

应用程序或服务的基本特征，如：

- 所使用的软件。
- 特殊的硬件要求。（有关更多信息，请参见本章后面的“ 确定高级功能的硬件兼容性 ”。）
- 数据量。
- 用户数量。

- 运行时间。

  对规模和性能的要求的预期变动，如：

- 季节性或其它计划的高峰负载。
- 用户的预期增长率。
- 数据的预期增长率。
- 在最初部署、高峰负载及项目规划各阶段的硬件要求。请根据应用程序和服务的特征及预期的变化估计这些要求。
- 应用程序、服务和操作系统的数据备份和灾难恢复计划。
- 最长停机容许时间（即，系统或用户可以容许的应用程序或服务无法使用的最长时间）。这很重要，因为消除所有可能的停机是代价很高的。 与进行更多的投资以保证高可用性相比，对许多应用程序和服务来说，偶尔短暂的停机也是可以接受的。
- 停机造成的影响。请定性地评估应用程序或服务的停机将对单位的哪些方面产生影响。这些影响可能包括，销售额损失、生产率降低、顾客满意度下降等。
- 停机造成的可测算的损失。请定量地估算每个应用程序或服务停机超过单位容许规定最大值所造成的损失。
- 识别规划的配置中存在的所有潜在故障点。
- 明确人员要求。
- 当前的可用性。如果还没有可用性的有关数据，请立即收集这些数据。从 Windows NT 4.0 SP4 开始，使用“ Microsoft Windows NT 4.0 服务器资源工具包 ”工具 Uptime.exe，可以很容易计算出系统正常运行时间。Uptime.exe 使用存储在事件日志中的事件计算这些数据。为此，必须先启用事件日志。“ Microsoft Windows 2000 Server 资源工具包 ”也提供了 Uptime.exe。

单故障点是指环境中，一旦发生故障，即会阻塞数据或应用程序的任何组件。

表 18.1 列出了服务器环境中常见的故障点，并说明了能否通过使用 Microsoft 群集解决方案或第三方解决方案保护这些故障点。

表 18.1 常见的故障点

故障点	群集解决方案	其它解决方案
网络集线器	N/A	冗余网络
网络路由器	N/A	OSPF
停电	N/A	- 提供不间断电源 (UPS) - 发电机 - 多电源阵列
服务器连接	故障转移	N/A

磁盘	故障转移	硬件或软件 RAID，以避免特定计算机上的特定数据丢失，并提供不间断服务
其它服务器硬件如 CPU 或内存	故障转移	备用组件如主板和小型计算机系统接口 (SCSI) 控制器（任何备用组件必须与原组件完全匹配，这包括网络和 SCSI 组件）。
服务器软件如操作系统或特定应用程序	故障转移	N/A
广域网 (WAN) 链接如路由器和专线	N/A	可以为远程连接提供辅助接入的冗余链接
拨号连接	N/A	多调制解调器及路由和远程访问

确定高级功能的硬件兼容性

请检查确认当前安装或计划购买的计算机系统和适配器已在 Microsoft 硬件兼容列表 (HCL) 中列出。要确定硬件是否已在 HCL 中列出并受支持，请参见 Web 资源页的“ Microsoft Windows Hardware Compatibility List ”链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources 。

如果您计划部署具有高级功能（如群集或大量的内存）的计算机系统，还有另外一些要求必须满足。

例如，如果有 RAM 在 4 GB 以上的 Advanced Server 计算机系统，您必须修改 Boot.ini PAE 开关，以允许使用 PAE 内存。可以在验证完所有组件都受支持之后进行这一修改。如果组件不受支持，必须让计算机系统符合要求，以避免潜在的问题。

如果在系统工作过程中添加新的适配器和驱动器，强烈建议您在做任何修改之前，先备份整个系统。

备注 对于可能引起计算机系统工作不正常或不稳定的注册表修改和 Boot.ini 文件的一些修改，可以通过在启动计算机时按下 F8 键加以避免，这样可绕过许多开关和驱动程序。然后可以对 Boot.ini 文件或其它区域进行必要的修改，以恢复功能。

确定群集要求

在确定了关键任务应用程序和服务对高可用性的特殊需求、识别了潜在的单故障点、并确定硬件与 Windows 2000 兼容之后，您必须确定哪类群集技术最适合本单位的需要。在规划群集之前，请先检查各项要求，以确定合适的群集类型。

规划网络负载平衡

网络负载平衡使用 TCP/IP 网络协议将一组运行服务器程序的计算机聚集在一起。网络负载平衡服务可以增强 Web 服务器、文件传输协议 (FTP) 服务器、流动媒体服务器、虚拟专用网络 (VPN) 服务器和其它关键任务程序的可用性和可扩展性。网络负载平衡让两台或更多主机（作为群集成员的服务器）一起工作，从而增强了这些功能。

运行 Windows 2000 Advanced Server 的单台计算机只能提供有限级别的服务器可靠性和可扩展性。而通过将两台或更多运行 Windows 2000 Advanced Server 的计算机资源并入一个群集，网络负载平衡就可以提供必需的可用性，保持 Web 服务器和其它关键任务程序的最佳性能。图 18.2 给出了一个包含四台主机的网

络负载平衡群集的例子。

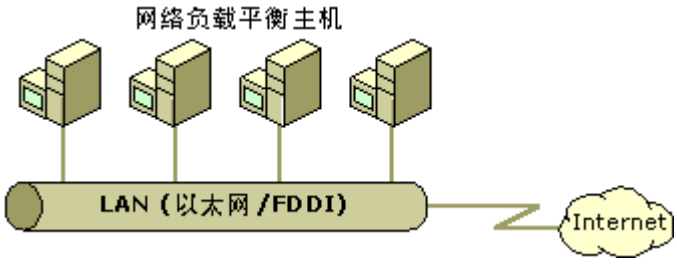


图 18.2 网络负载平衡群集中的四台主机

每台主机都运行服务器程序（如 Web 服务器、FTP、Telnet、和通信）的一个独立副本；对有些服务，如 Web 服务器，程序的副本运行在群集内所有主机上，而网络负载平衡在这些服务器之间分配工作量。对其它一些服务，如通信，将只有一个服务副本负责处理群集内的工作。与平均分配这些服务负载不同，网络负载平衡让网络通信流向一台主机，并只在服务器发生故障时，才将该通信移到其它主机。网络负载平衡允许群集中的所有计算机都使用同一组群集网际协议（IP）地址被寻址—— 同时又保留了各自现有的专用 IP 地址。网络负载平衡在各主机间分配入站的客户请求，如 TCP/IP 通信，包括 TCP 连接和 UDP 流。

为了均衡服务器性能，网络负载平衡将入站的 TCP/IP 连接负载在群集中所有主机之间平衡分配。如果需要，您可以配置每台主机的负载大小。还可以动态地将主机添加到群集，以应付负载的增加。另外，网络负载平衡可以将所有的 TCP/用户数据报协议（UDP）通信引入指定的一台主机（不配置为负载平衡），该主机称为“默认主机”。这样也有好处的，因为它允许没有明确配置为负载平衡的所有服务在单一主机上运行。网络负载平衡会管理 TCP/IP 通信，以保持服务器程序的高可用性。

当一台主机发生故障或脱机时，网络负载平衡将自动重新配置群集，将客户请求重定向到其它计算机。对于负载平衡程序，负载会在仍在运行的计算机之间自动重新分配。 对于运行于单一服务器的程序，则将其通信重定向到指定的另一台主机。与发生故障的或脱机的服务器的连接将断开。在完成了必要的维护之后，脱机的计算机可以显式地重新加入群集并获得本来属于它的那份工作。

网络负载平衡不会检测应用程序故障。相反，它被设计成受应用程序监视程序的控制；监视程序会检查并确保相应的应用程序行为正常。例如，如果应用程序监视程序确定服务发生了故障，它会命令网络负载平衡从群集中移走受影响的主机，直到问题得到纠正。另外，网络负载平衡还检测群集主机是否正常关机及网卡有否发生故障。

如果您提供的 TCP/IP 主机服务（如 Web 服务器）必须维持其性能且连续可用，才能满足日益增长的客户需求，那么就需要有网络负载平衡。例如，Internet 电子商务站点面临爆炸式增长的需求，在这些站点，发生停机对顾客来说是不能接受的。单靠传统的均衡服务的方法，如使用循环域名系统（DNS），已经无法提供象网络负载平衡那样的高可用性。循环 DNS 是一个可以为 Web 服务器提供有限的 TCP/IP 负载平衡的解决方案。

规划网络负载平衡群集的过程

本节讨论了在规划本单位的网络负载平衡群集时必须考虑的一些指导方针。在规划网络负载平衡群集时，不妨考虑使用图 18.3 流程图给出的规划过程。

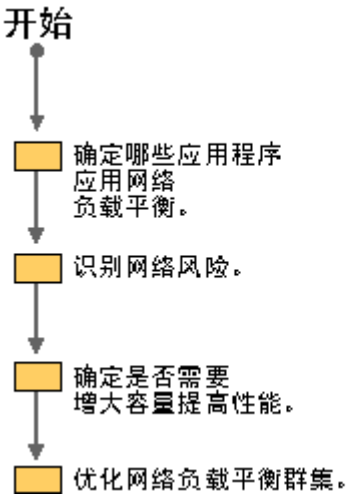


图 18.3 规划网络负载平衡群集的过程

确定哪些应用程序应用网络负载平衡

许多应用程序都可以与网络负载平衡一起运行。本节提供的指导方针可以确定哪些应用程序适合负载平衡。

一般来说，网络负载平衡能够均衡所有使用 TCP/IP 网络协议，并与特定 TCP 或 UDP 端口关联的应用程序或服务。

网络负载平衡使用“端口规则”；该规则说明了哪些通信需要平衡负载，而哪些通信可以忽略。默认时，网络负载平衡将所有端口配置为负载平衡。但您可以修改这一配置，确定入站网络通信在各端口如何平衡负载。要修改默认行为，可以创建一个包括特定端口范围的端口规则。

下面是一些服务及其相应端口的例子：

- TCP/IP 上的 HTTP：Web 服务器，如 Microsoft Internet 信息服务 (IIS):端口 80。
- TCP/IP 上的 HTTP：安全套接层 (SSL) 上的 HTTP，用于加密 Web 通信:端口 443。
- TCP/IP 上的 FTP：FTP：端口 21、端口 20、和端口 1024-65535。
- TCP/IP 上的 TFTP：次要文件传送协议 (TFTP) 服务器,用于引导协议 (BOOTP) 之类的应用程序：端口 69。
- TCP/IP 上的 SMTP： 简单邮件传输协议 (SMTP),用于 Microsoft Exchange 之类的应用程序：端口 25。
- Microsoft 终端服务：端口 3389。

要成功地平衡负载，应用程序或服务必须设计成允许多个例程（程序的多个副本）同时运行，每台群集主机上运行一个副本。例如，如果没有明确提供一种方法，应用程序将不能更新一个反过来将被其它例程更新的文件。为了避免这一问题发生，请安装一台后端数据库服务器，以处理对共享信息的同步更新。

另外，网络负载平衡通常用于：

- VPN 服务器

  VPN 服务器负责为专用网络的扩展提供服务；专用网络扩展负责将链接覆盖到共享或公用网络（如

Internet）。

- 流动媒体服务器

  提供多媒体支持的软件（如 Microsoft Media Technologies），允许您在 Intranet 或 Internet 上使用 Advanced Streaming Format（高级流动格式）传送内容。

如果断定单位将会从负载平衡 PPTP 或流动通信中获益，那么网络负载平衡将不失为 VPN 服务器和流动媒体服务器的上佳选择。

备注 在网络负载平衡群集中进行应用程序的负载平衡之前，请检查应用程序许可或与应用程序供应商核实。每个应用程序供应商都为在群集中运行的应用程序设置了不同的授权策略。

在 VPN 服务器上使用网络负载平衡来平衡 PPTP 客户负载时，很重要一点是正确配置 TCP/IP 属性，确保与运行 Windows 早期版本（例如，Windows 98 和 Windows NT 4.0）的客户兼容。为此，请只为那些网络负载平衡用到的网卡分配一个虚拟 IP 地址，并在这个子网上不再分配专用 IP 地址。这一限制不适用于 Windows 2000 客户。

有关为 VPN 和其它应用程序配置网络负载平衡的更多信息，请参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide* 中的“Windows Clustering”。

使用网络负载平衡部署终端服务器群集

当配置为“应用程序服务器”模式时，Windows 2000 终端服务可以为远程用户集中部署和执行应用程序。您可以使用网络负载平衡在一组终端服务器之间分配大的客户群。这最适合的情况是，终端服务器应用程序在很大程度分散于不同的地方，比如为销售人员或仓库提供的数据输入应用程序。

如果当前的终端服务器会话需要漫游用户不断的重新连接，就不能使用网络负载平衡提供完美的漫游体验。由于网络负载平衡将根据 IP 地址把用户路由到群集主机，因此从多个位置连接的用户或使用 DHCP 并在会话间隙断开连接的用户并不总是被路由回同一台计算机，因此也就不能重新匹配断开的会话。即使这种情况，网络负载平衡也能为掉线会话提供重新连接，或为 IP 地址固定的用户提供持续的路由。如果不要求保持切断的会话，您就可以将网络负载平衡有效地用于任何种类的终端服务器应用程序。

在使用网络负载平衡时，建议您将所有终端服务器配置成，在适当的超时（如 30 分钟）之后结束断开的会话。这种配置允许掉线会话恢复，但不允许断开会话持续很长时间。持续的会话在用户被路由到其它计算机时会出现问题，因为计算机没有重新连接。这种配置为每个用户将会话留在多个计算机上，因而消耗了资源，最糟糕的情况是用户可能被拒之门外，因为他们的资源正在其它地方使用。

在使用网络负载平衡部署终端服务群集时，每台服务器都需要能够为所有用户提供服务。为此，必须将每个用户的信息、系统信息以及公用数据存储在可访问的地方，如后端文件服务器。图 18.4 给出了网络负载平衡和终端服务的一种实现形式。

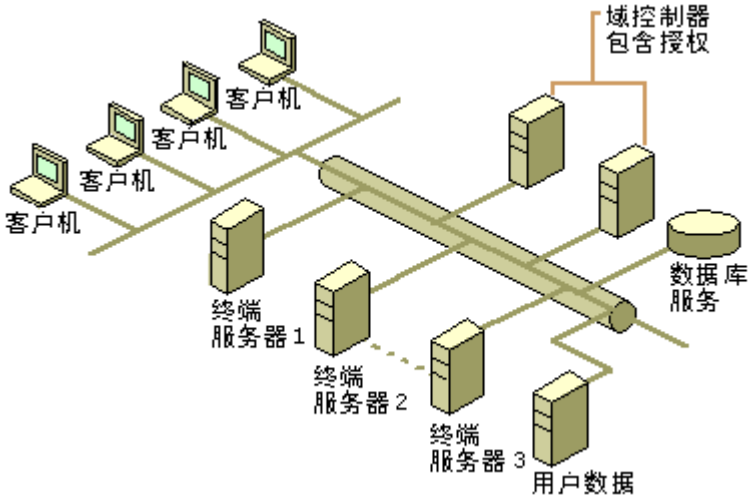


图 18.4 网络负载平衡在终端服务器之间提供平衡

注意服务器将分别负责业务流数据库应用程序及每用户数据存储。这些服务器中的每一台都必须使用群集或其它合适技术实现高可用性。另外，可用性的提高也将通过分散工作量提高可扩展性，使多个终端服务器满足需要的性能水平。

有关终端服务的更多信息，请请参见本书的“ 部署终端服务 ”。

为运行 IIS/ASP 和 COM+ 应用程序的服务器配置网络负载平衡群集

电子商务站点的一个关键组件是运行 COM+ 应用程序的服务器。在如图 18.5 所示的示例中，运行 COM+ 的服务器负责为网上书店的购物篮处理对象请求。

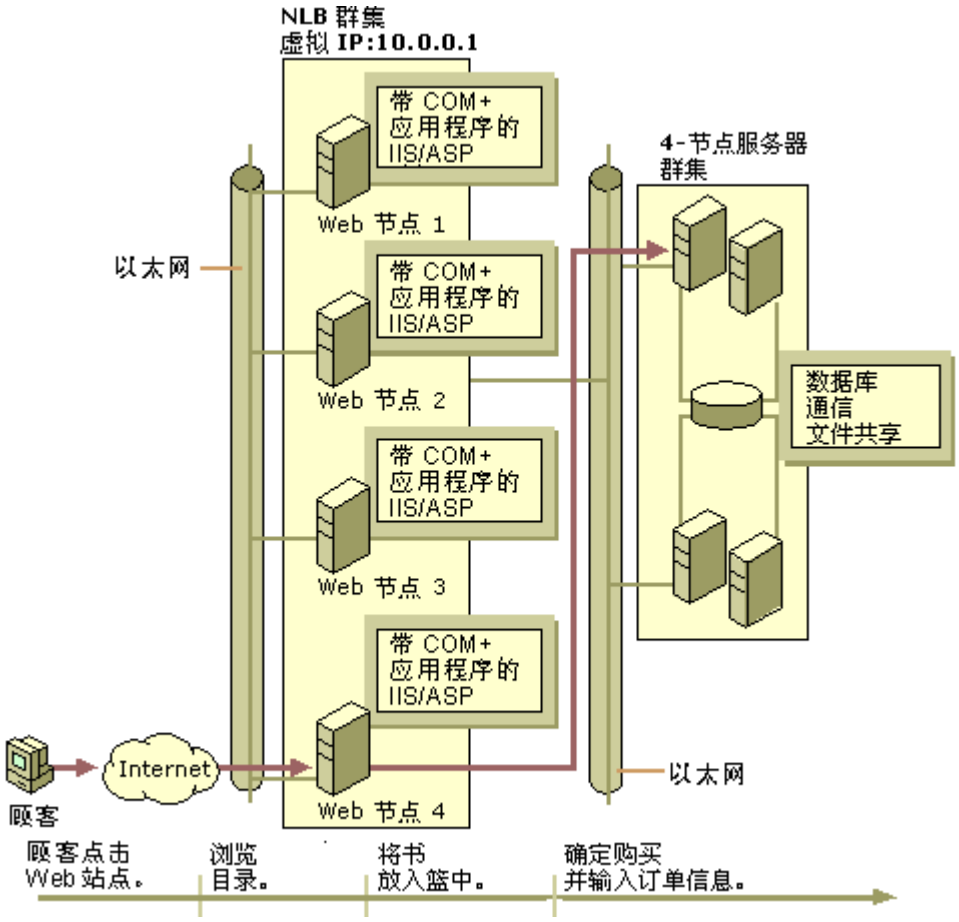


图 18.5 与 IIS 在同一的物理服务器上部署 COM+ 应用程序

为了保证在需要时这些对象可用，并使站点的整体性能最大化，建议您将 COM+ 与 IIS 部署在同一物理服务器上。这样，应用程序服务器可以利用现有的网络负载平衡群集增加的可扩展性和可用性，而无需额外单独运行 COM+ 专用服务器队列。

使用为 IIS/ASP 和 COM+ 配置的单个物理网络负载平衡服务器群集，与单独建立应用程序服务器物理队列相反，可以降低硬件和管理开销，因为这只需要更少的服务器

识别网络风险

在识别网络风险时，应该确定引起网络资源访问中断的可能故障。单故障点可以包括硬件、软件或外部相关因素，如市政公司的电源供给或专用广域网 (WAN) 线路。

一般，在下列情况下您可以提供最大的可用性：

- 将环境中的单故障点数量降到最少。
- 提供故障发生时的服务维护机制。

如果使用网络负载平衡，在下列情况下您也可以提供最大的可用性：

- 只平衡那些适合网络负载平衡的应用程序的负载。

- 确保应用程序服务器已为所运行的应用程序正确配置。有关正确配置的更多信息，请参见本章后面的“ 确定服务器容量要求 ”。

网络负载平衡的主要目标是提高可用性。两台或更多计算机的群集可以保证如果一台计算机发生故障，另一台计算机可继续处理客户请求。但网络负载平衡并没有设计成在任何情况下都能保护工作流的方方面面。例如，网络负载平衡并不是备份数据的替代方案。网络负载平衡只保护对数据的访问，而不是数据本身。同时，它不能防止导致整个群集停用的停电现象。

Windows 2000 Advanced Server 有几个内建功能，可以在发生故障时保护某些计算机和网络进程。这些功能包括：独立磁盘冗余阵列 (RAID) 1（磁盘镜像）和 RAID 5（带奇偶校验的磁盘分条）。在规划网络负载平衡环境时，请明确这些功能可在哪些地方帮助您，而网络负载平衡却不能。

规划网络负载平衡

本节将帮助您确定单位需要的网络负载平衡服务器的数量，以及需要如何配置它们。

群集大小（定义为参加群集的群集主机的数量，Windows 群集可有多达 32 台主机）要根据满足对某个应用程序预期客户负载所要求的计算机数量来确定。

例如，如果您确定需要六台计算机运行 IIS 才能满足对 Web 服务的预期客户需求，网络负载平衡将在所有六台计算机上运行，则群集就包括六台群集主机。

通常的规则是，一直添加服务器，直到群集能轻松地处理客户负载而不会超载。需要的最大群集规模取决于给定子网的网络容量。准确的数量则取决于应用程序的性质。

备注 一定要确保有足够的多余服务器容量，这样如果一台服务器发生故障，其余的服务器能够适应负载的增加。

当群集子网接近网络的饱和状态时，请在不同的子网上再添加另外一个的群集。并使用循环 DNS 将客户引到该群集。当网络需求增长时，您可以继续以这种方式添加群集。由于循环 DNS 只包含群集 IP 地址，客户始终被引向群集，而不是分立的服务器，从而决不会由于一台服务器发生故障而造成停机。在一些要求高带宽的部署中，您可以使用循环 DNS 将入站通信在多个相同的网络负载平衡群集之间拆分。图 18.6 中，IP 请求找到 DNS (www.reskit.com)，而 DNS 负责解析到网络负载平衡群集 1 的虚拟 IP 地址 (10.0.0.1) 并将请求传递给网络负载平衡群集。然后，随后的请求被发送到群集 2 (10.0.0.2) 和群集 3 (10.0.0.3)，然后以循环方式继续下去。

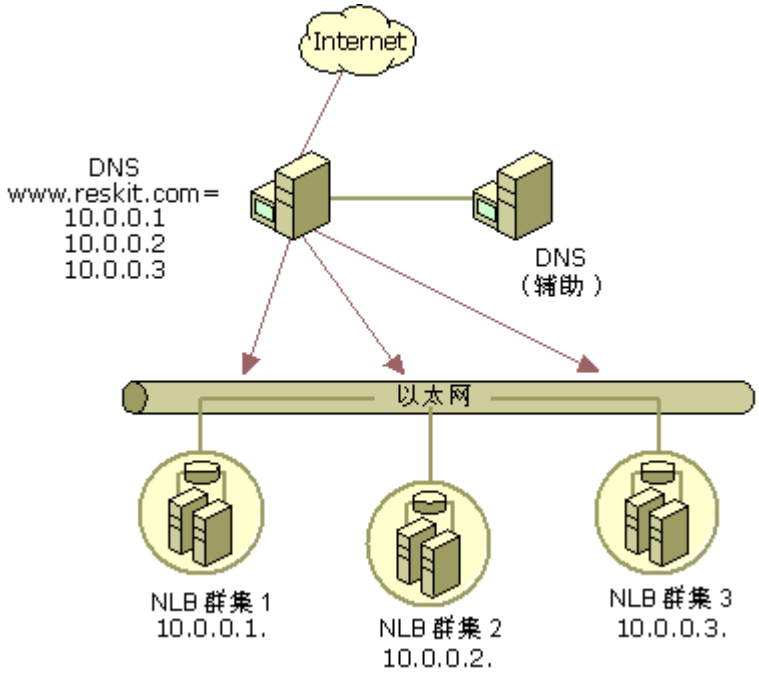


图 18.6 完全相同的网络负载平衡群集之间的循环 DNS

备注 如果使用了网络交换机并部署了两个或更多群集，请考虑将各群集放在不同的交换机上，这样入站群集通信会得到分别处理。“交换机”用于将群集主机连接到路由器或其它入站网络连接源。

很重要一点是，注意在有多个群集时，交换机可用来分开入站通信。

确定服务器容量要求

在确定了群集大小之后，便可以开始分别配置各台群集主机了。一般来说，您做出的决定应该基于计划平衡负载的应用程序类型，以及客户对应用程序的预期需求。一些服务器应用程序，如文件和打印服务器相当消耗磁盘，因而要求非常大的磁盘容量和快速的输入输出（I/O）。请务必查阅每个应用程序的相关的资料，以确定如何配置群集中的服务器。

虽然可以用两三台功能非常强大的服务器代替数量较多、功能稍弱的计算机，但通常部署多台计算机更为理想。使用较多的服务器可以让客户负载更加广地分布，这样如果一台服务器发生故障，对客户的负面影响将会减少。

优化网络负载平衡群集

有一些硬件和配置可以提高群集网络负载平衡的性能。这些将在以下几节讲述。

如果群集主机直接连到交换机接收客户请求，入站客户通信会自动发送至所有交换机端口。在大多数应用程序中，入站客户通信是总群集通信的很小一部分。但如果其它群集或计算机也连接到同一交换机上，这种群集通信会消耗一些端口带宽。

为了避免这种问题，您可以将所有群集主机连接到集线器或中继器，集线器或中继器再上行连接到单个交换机端口。这样，所有入站客户通信将从集线器或中继器流向单个交换机端口，同时传送到所有群集主机。如果客户通信从多个上游交换机端口到达交换机，您可以为每台连接到单个交换机端口的主机添加第二专用网卡。在群集子网的每台主机上使用两个网卡有助于将网络通信引导通过各群集主机。入站客户通信流经交换式集线器到达所有主机，而出站通信则直接流向交换机端口。

网络负载平衡要求

在以下几个条件满足时，应用程序可在网络负载平衡群集上运行：

- 与客户的连接必须配置为使用 IP。
- 要平衡负载的应用程序必须使用 TCP 或 UDP 端口。
- 应用程序多个完全相同的例程必须能够在分立的多个服务器上同时运行。如果应用程序的多个例程共享数据，必须有一种方法使其更新同步。

网络负载平衡被设计成 Windows 2000 Advanced Server 下的标准网络设备驱动程序。因为网络负载平衡是为基于 TCP/IP 的服务器程序提供群集支持的，所以必须安装 TCP/IP 才能利用网络负载平衡功能。目前版本的网络负载平衡在群集内的光纤分布式数据接口 (FDDI) 或基于以太网的局域网上工作。它在很多不同网卡的 10 兆字节/秒 (Mbps)、100 Mbps 和 GB 以太网网络上都成功地经过了测试。

网络负载平衡占用不到 1 兆字节 (MB) 的存储空间，以默认参数内运行时，视网络负载情况的不同，将使用 250 千字节 (KB) 到 4 MB 的 RAM。您可以修改默认参数，以允许使用高达 15 MB 的内存。典型的内存使用量介于 500 KB 和 1 MB 之间。

要优化群集性能，可以在每台网络负载平衡主机上安装第二网卡，以处理寻址到（作为网络中单一计算机的）服务器的网络通信。在这种配置中，启用网络负载平衡所针对的第一块网卡，负责处理寻址到（作为群集的一部分的）服务器的客户网络通信。虽然不要求第二网卡，但如果有，则可以提高网络的总体性能，例如访问后端数据库的性能。当网络负载平衡处于默认单播模式时，就需要第二块网卡负责群集内服务器之间的通信，例如服务器之间的文件复制。

有关系统要求及群集和主机参数的更多信息，请参见 *Distributed Systems Guide* 中的“Windows Clustering”。

使用路由器

网络负载平衡可以两种模式运行：单播和多播。 默认状态将启用单播支持，以保证所有路由器都能正常工作。可以选择了启用多播模式，在群集内通信就不需要第二网卡。如果网络负载平衡客户通过路由器访问群集（配置为多播模式），要确保路由器可以接受对群集（单播） IP 地址的地址解析协议 (ARP) 应答，（其中这些（单播）IP 地址带有一个 ARP 结构有效载荷范围内的多播媒体访问控制地址）。ARP 是一项 TCP/IP 协议，使用到本地网络的有限广播解析逻辑上分配的 IP 地址。

这就允许路由器将群集的主 IP 地址和其它多宿主地址，映射到相应的媒体访问控制地址。如果您的路由器不满足这种要求，可以在路由器中创建一个静态 ARP 项目，也可以在默认单播模式下使用网络负载平衡。

一些路由器会要求静态 ARP 项目，是因为它们不支持将单播 IP 地址解析为多播媒体访问控制地址。

规划群集服务

Windows 2000 Advanced Server 中的群集服务为服务器群集提供了基础。当群集中的一台服务器发生故障或脱机时，群集中的另一台服务器将接管故障服务器的工作。使用服务器资源的客户几乎不会感觉到他们的工作有停顿，因为资源支持已从一台服务器转移到其它服务器。

在服务器群集中，群集服务负责管理所有群集特定的活动。这里有一种情况是群集服务运行于群集的所有节点上。特别是，群集服务会处理以下工作：

- 管理群集对象、群集磁盘和配置。
- 与群集中的其它群集服务例程协调。
- 执行故障转移操作。
- 处理事件通知。
- 促进其它软件组件间的通信。

下列情况下，将要求使用服务器群集：

- 用户依赖于经常对业务关键数据和应用程序的访问才能完成工作。
- 您不能接受超过 30 分钟的服务停机（未计划的或计划的）。
- 备份服务器的费用低于发生故障时让业务关键数据和应用程序脱机的损失。

备注 术语“备份服务器”通常意味着保持一台服务器空闲，直到需要时才开始工作。虽然可以这样配置，但这不是服务器群集的主要目标。

规划服务器群集的过程

本节讨论了规划单位的服务器群集时需要考虑的指导方针。不妨考虑使用图 18.7 所示的规划过程。

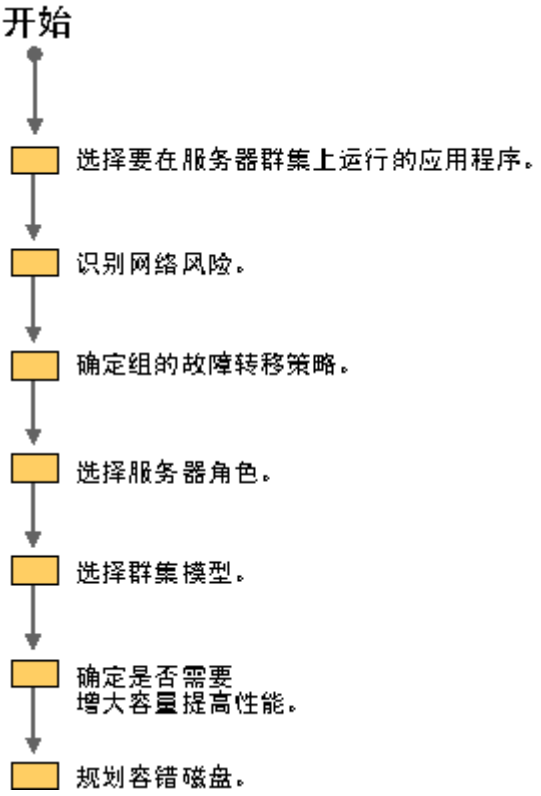


图 18.7 规划服务器群集的过程

选择运行于服务器群集的应用程序

您可以将任何应用程序部署运行在群集中的任何服务器上；但不是所有的应用程序都能故障转移。在那些能够故障转移的应用程序中，也不是所有的都需要设置为群集资源。本节提供了做出这些决定的指导方针。

下列标准将帮助您确定一个应用程序是否适应服务器群集故障转移机制：

- 客户机和服务器应用程序必须使用 TCP/IP （或分布式组件对象模型、命名管道或 TCP/IP 上的远程过程调用）进行网络通信，以在服务器群集上运行。只使用 NetBIOS 增强型用户接口 (NetBEUI) 或网际数据包交换 (IPX) 协议的应用程序将不能利用群集故障转移。
- 应用程序必须能指定应用程序数据存储在什么地方。

  在服务器群集上运行的任何应用程序必须能够将其数据存储在一个可配置的位置，也就是说，存储在与共享磁盘总线连接的磁盘上。一些不能将其数据存储在可配置位置的应用程序仍可以配置为故障转移。但这种情况下，对应用程序数据的访问在故障转移时会丢失，因为数据只在故障节点的磁盘上可用。这种情况下，这些数据在群集中节点间的复制，也许会有所帮助。
- 在发生故障时，应用程序可以重新启动。
- 可以在群集中所有节点上安装该应用程序。
- 发生暂时的网络故障时，连接到服务器应用程序的客户应用程序必须重试从中恢复。

  在故障转移时，客户应用程序将感觉到暂时失去网络连接。如果将客户应用程序配置为从暂时的网络连接问题恢复，在服务器故障转移之后，它就可以继续运行。

可以将能故障转移的应用程序分成两组：使用群集 API 的组和不使用群集 API 的组。

支持群集 API 的应用程序定义为“ 支持群集型 ”。这些应用程序可以用群集服务注册成接收状态和通知信息，并可以使用群集 API 管理群集。

不支持群集 API 的应用程序被定义为“ 不支持群集型 ”。如果不支持群集型应用程序满足 TCP/IP 和远程存储标准，也可以在群集中使用它们，并常可以配置为故障转移。

不论哪种情况，在内存中保留重要状态信息的应用程序不是最适合用于群集的应用程序，因为不存储在磁盘上的信息在故障转移时将会丢失。这种结果类似于重新启动了服务器或服务器遇到电源故障。

识别网络风险

在配置群集时，请识别会引起网络资源访问中断的可能故障。单故障点可以是硬件、软件或外部相关因素，如市政公司的电源供给和专用广域网 (WAN) 线路。

一般来说，在下列情况下可提供最大的可用性：

- 将环境中的单故障点数量降到最低。
- 提供故障发生时的服务维护机制。

有了 Windows 2000 Advanced Server，您就能用服务器群集和新的管理程序来提供更高的可用性。然而，服务器群集没有设计成可以在任何情况下保护工作流的所有组件。例如，群集不是备份数据的替代方案；它们只保护数据的可用性，而不是数据本身。

Windows 2000 Advanced Server 有几个内建功能，可以在发生故障时保护某些计算机和网络进程。这些功能包括：镜像 (RAID 1) 和奇偶校验磁盘分条 (RAID 5)。在规划群集时，请确定这些功能可以在哪些地方帮助您，而服务器群集却不能。

备注 Windows 2000 逻辑卷管理器提供的软件 RAID 不能用来保护群集服务管理的磁盘。请使用硬件 RAID 保护这些磁盘。

为了进一步提高网络资源的可用性并防止数据丢失，不妨考虑以下事项：

- 在站点中保证有可用的替换磁盘和控制器。一定要确保您手头的任何备用部件都与原件完全匹配，其中包括网络和 SCSI 组件。与让几百个客户不能使用数据的代价相比，两个备用 SCSI 控制器的费用微不足道。
- 为计算机和网络本身（包括集线器、网桥、和路由器）分别配备不间断电源 (UPS) 保护。UPS 设备使用电池使计算机在停电之后能继续运行一段时间。运行 Windows 2000 Server 的计算机支持 UPS。UPS 解决方案必须为操作系统提供足够长时间的供电，以在电源故障时完成正常关机。

确定资源组的故障转移和故障回复策略

“ 资源组 ”是指非独立的或相关的资源的集合。非独立资源需要其它资源才能顺利工作。单个资源不能独立地故障转移。同一资源组中，资源将和其它所有资源一起故障转移。

您可以为群集中的每个资源组指定故障转移策略。“ 故障转移策略 ”会完全确定发生故障转移时，组如何进行操作。您可以为设置的每个资源组选择其最适合的策略。

组的故障转移策略包括三项设置：

故障转移时间

可以将组设置为当影响该组的资源发生故障时立即故障转移，也可以指示群集服务尝试重启故障资源一定次数之后再启动故障转移。如果资源故障有可能通过重启组内的所有资源加以克服，那么请将群集服务设置为重新启动该组。

首选节点

您可以这样设置一个组，让它一旦指定的节点可用，就在其上运行。这在其中一个节点的装备对于为组提供主机更有利时，很有用处。注意这种设置只在由于节点故障发生故障转移时生效。否则，必须手动为资源组提供主机的节点。

故障回复时间

故障回复是指，在首选节点发生故障但又回到联机状态之后，将资源重新移回首选节点（以单个或以组的形式）的过程。

您可以将组配置成一旦群集服务检测到发生故障的首选节点已经还原，就马上故障回复到该首选节点；也可以让群集服务待到一天的特定时间，比如在高峰访问时间之后进行故障恢复。

有关规划资源组的更多信息，请参见本章后面的“ 规划资源组 ”。

选择服务器角色

服务器群集中的节点，可以是成员服务器，也可以是域控制器。但不论哪种情况，两种节点都必须属于同一域。

如果将群集节点配置为域控制器，必须首先保证有硬件支持它们。有关更多信息，请参见本章后面的“ 确定群集服务的容量要求 ”。

如果将所有的群集节点都配置为成员服务器，那么群集的可用性将取决于域控制器的可用性。只有域控制器可用时，群集才可用。请规划足够的域控制器，以达到要求的可用性等级。有关提高可用性的更多信息，请参见本章前面的“ 识别网络风险 ”。

您必须考虑域控制器服务产生的额外开销。在运行 Windows 2000 Advanced Server 的大型网络中，域控制器需要充足的资源，以执行目录复制及为客户做服务器身份验证。因此，为了达到最佳性能，许多应用程序，如 SQL Server 和消息队列，都建议在域控制器上不再安装其它应用程序。但如果网络非常小，上面的帐户信息很少变动，用户不经常登录和注销，可以使用域控制器作为群集节点。

选择服务器群集模型

依照复杂程度，服务器群集可以分为三种配置模型。本节介绍了每种模型，并给出了适合每种模型的一些类型的应用程序示例。这些模型可以是单个节点的群集，也可以是所有服务器都提供服务的群集。请选择最能满足本单位需要的群集模型。

模型 1：单节点服务器群集配置

模型 1 说明了如何在单节点服务器群集运行应用程序的虚拟服务器概念。

这种群集模型不使用故障转移。这只是为了方便管理和方便客户在服务器中组织资源的一种方法。这一模型的主要优点在于，管理员和客户两者都能随时看到网络上的带有描述性名称的虚拟服务器，而不必浏览实际服务器的列表才能找到需要的共享资源。

这种模型的其它优点包括：

- 在资源发生故障但计算机又被恢复之后，群集服务会自动重启各种应用程序和非独立资源。这对于那些能够从自动重启功能获益但自己却没有这种机制的应用程序很有用。
- 您可以将单一节点与第二个节点在未来某个时间组成群集，而资源组已经就位。为组配置了故障转移策略之后，虚拟服务器便可以开始工作。

图 18.8 给出了一个不使用故障转移的单节点群集的例子。

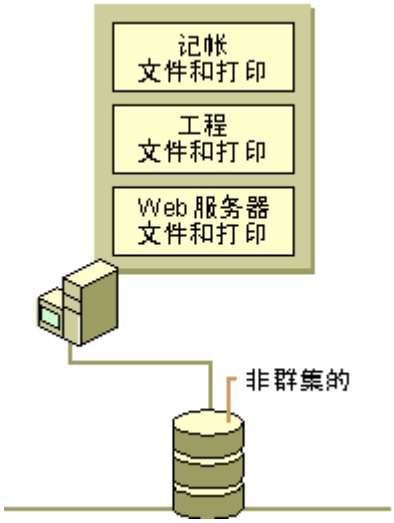


图 18.8 单节点服务器群集配置

例如，可以使用这一模型将所有的文件和打印资源放在一台计算机上，而为每个部门分别建立组。当一个部门的客户需要连接到适当的文件或打印共享时，找到共享就如同找到一台实际的计算机一样容易。

备注 有一些应用程序（如 SQL Server 6.5 和 7.0 版），不能安装在单节点群集上。

模型 2：专用辅助节点

模型 2 为资源提供了最大的可用性和最好的性能，但它要求为大部分时间不使用的硬件进行投资。

一个节点（称为“主节点”）支持所有的客户机，而其伙伴节点却空闲。伙伴节点是专用于一旦主节点发生故障转移便准备好可以使用的服务器。如果主节点发生故障，专用辅助节点立即接管所有操作，并继续以接近或等同于主节点的性能为客户机服务。这种方法常常称为主动/被动配置。准确的性能将取决于辅助节点的容量。图 18.9 给出了一个专用辅助节点的例子。

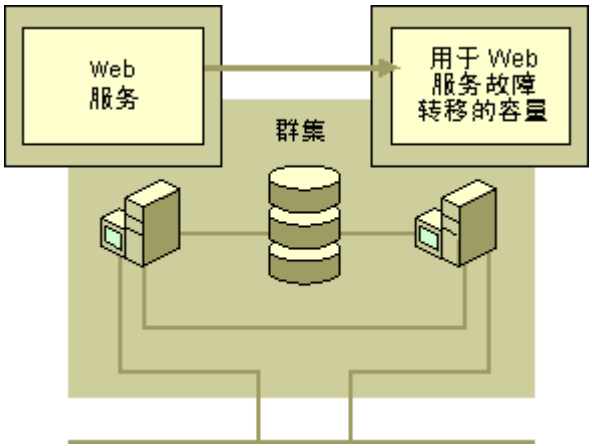


图 18.9 主动/被动配置

模型 2 最适于单位中最重要的应用程序和资源。例如，如果您的单位依赖通过万维网进行销售，您就可以使用这一模型为所有专门支持 Web 访问的服务器提供辅助节点，比如那些运行 Internet 信息服务 (IIS) 的服务器。这种情况下重复配置硬件的费用是合理的，因为它能够保护客户对本单位的访问。如果其中一台 Web 服务器发生故障，另一台服务器已经配置完备，可以接管其操作。

如果您的预算允许为主节点配备容量相同的辅助服务器，那么对任何组，都不必设置首选服务器。如果一个节点的容量比另一个大，那么，将组故障转移策略设置成首选较大的服务器，就可以保持性能尽可能高。

如果辅助节点容量与主节点容量完全相同，请将策略设置成防止所有组故障回复。如果辅助节点容量比主节点容量少，请将策略设置成立即故障回复或在指定的非高峰时间故障回复。

部署示例：主动/被动拆分配置

主动/被动拆分配置给出了专用辅助节点的例子。主动/被动拆分配置说明，服务器群集中的节点不仅限于提供使用群集的应用程序。提供群集资源的节点也可以提供如果服务器停止工作将停止的不支持群集型的应用程序。

规划资源组的步骤之一是，明确将不配置为故障转移的应用程序。那些应用程序可以驻留在构成群集的服务器上，但必须在本地磁盘上而不是共享总线的磁盘上存放数据。 如果这些应用程序的高可用性很重要，必须找到提供这种高可用性的其它方法。图 18.10 给出了一个主动/被动拆分配置的实例。

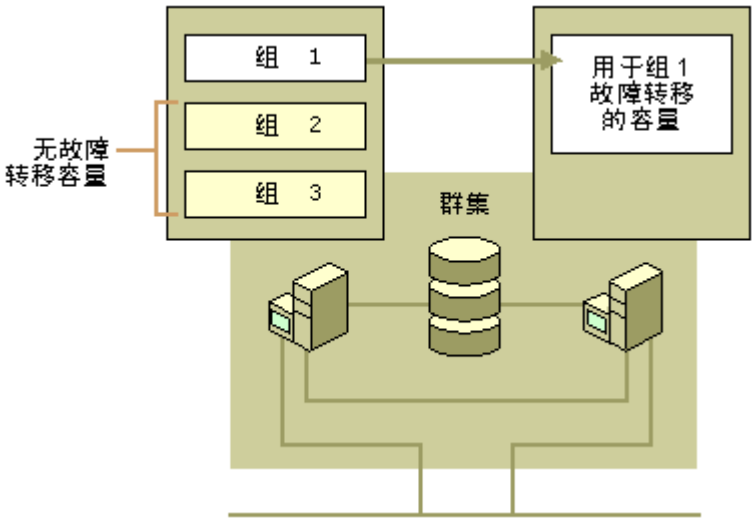


图 18.10 主动被动拆分配置

其它组的应用程序也在一台服务器上为客户提供服务，但因为它们是不支持群集的，所以不要为它们建立故障转移策略。例如，您可以让节点运行不使用故障转移的邮件服务器，或那些不经常使用以至可用性并不重要的记帐应用程序。

节点发生故障时，没有用故障转移策略配置的应用程序将不可用，除非它们自己有内建的故障转移机制。它们会保持这种不可用状态，直到节点还原；您必须手动重启它们，或者将 Windows 2000 Advanced Server 设置成在系统软件启动时自动启动它们。用故障转移策略配置的应用程序则根据策略照常故障转移。

模型 3：高可用性配置

模型 3 在只有一个节点联机时，可以提供可靠性和可以接受的性能，并在两个节点同时联机时，提供高可用性和高性能。这种配置能够最大限度地使用硬件资源。

在这个部署的例子中，每个节点使其自己的资源组以虚拟服务器的形式对网络可用，其中虚拟服务器可以被客户检测和访问。服务器群集中，“ 虚拟服务器 ”是一组资源，包括网络名称资源和 IP 地址资源，它们包含在资源组中。每个节点的容量都被选择成，每个节点上的资源都以最佳的性能运行；但如果发生故障转移，任何节点都可以临时接管运行资源的负担。视资源和服务器容量配置的不同，所有的客户服务在故障转移时和故障转移之后仍然可用，但性能会有所下降。图 18.11 给出了一个主动/主动配置的示例。

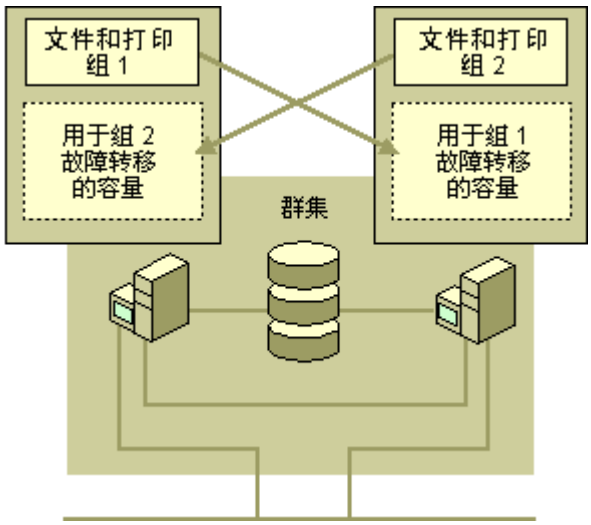


图 18.11 主动/主动配置

例如，您可以将这种配置用在专用于文件共享和打印后台处理服务的群集。多个文件和打印共享被组成为一些独立的组，一个节点上一个。如果一个节点发生故障，其它节点会临时接管所有节点的文件共享和打印后台处理服务任务。被临时重新安置的组的故障转移策略设置为首选原节点。故障节点还原后，被重新安置的组将返回到其首选节点的控制之下，且运行恢复到正常性能。在整个过程，服务始终可用，只有微不足道的中断。

以下部署示例给出了一些类型的高可用性配置。

部署示例 1:单一应用程序类型群集

本例说明了如何解决大型计算环境中通常发生的两个挑战。第一个挑战发生在由单一服务器运行多个大型应用程序，引起网络性能下降时。为了解决这一问题，请用一台或更多服务器与第一台服务器组成群集，并将应用程序在几台服务器之间拆分。

第二个挑战发生在在分立的服务器上运行相互关联的应用程序时。当服务器没有连接时，就会产生可用性问题。通过将它们放入群集，将能为客户保证两种应用程序都有较高的可用性。

假设您的公司 Intranet 依赖一台运行两个大型数据库应用程序的服务器。这两个数据库对一天到晚不断连接到此服务器的几百个用户都至关重要。这里的挑战将是，在高峰连接时间服务器不能满足需求，性能常常下降。

通过将第二台服务器连接到超载的服务器，构成群集并平衡负载，可以使这一问题得到缓解。现在，您有了多台服务器，每台服务器运行一个数据库应用程序。如果一台服务器发生故障，可能会感到性能有所下降，但只是短暂的。当故障服务器恢复后，它运行的应用程序将故障回复，并重新运行。图 18.12 给出了这一解决方案。

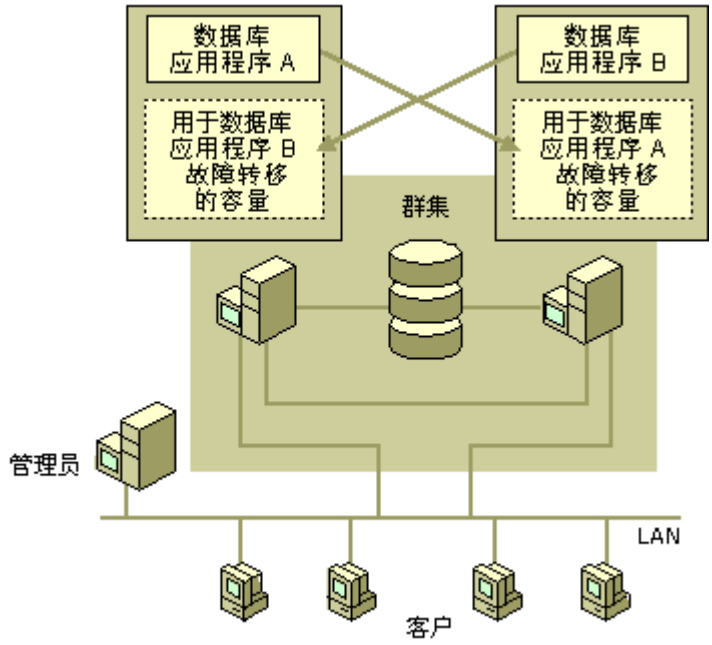


图 18.12 将另一台服务器连接到超载的服务器构成群集

部署示例 2:多个应用程序的群集

假设您的零售业务依赖两个分离的服务器，一台负责提供通信服务，另一台为产品清单和定单信息提供数据库应用程序。

两种服务对业务来说都必不可少。员工依赖通信服务进行日常业务管理。而如果不能访问数据库应用程序，顾客将不能放置订单，员工也不能访问产品清单或运送信息。图 18.13 是当关键任务应用程序和服务依赖分立的服务器，从而将应用程序和服务置于危险境地的典型配置。

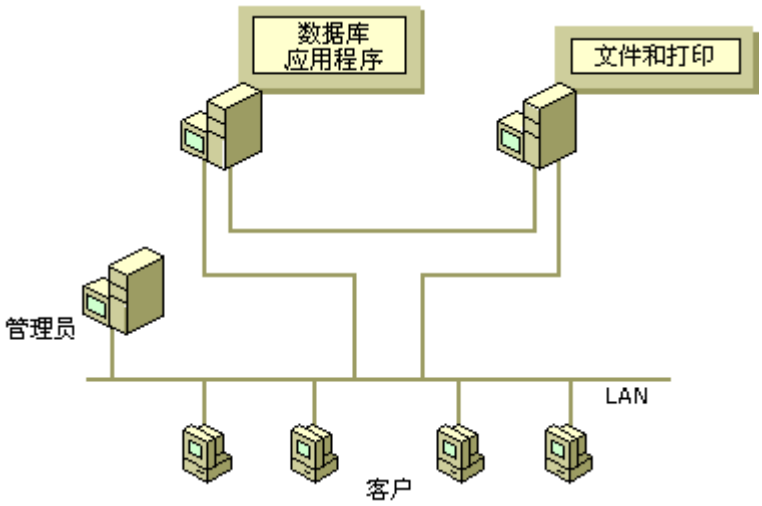


图 18.13 关键任务应用程序和服务依赖分离的服务器

为了确保所有服务的可用性，请将计算机组合成群集。

可以创建包含两个组的群集，每个节点上一个组。一个组包含运行通信应用程序需要的所有资源，而另外一个组包含数据库应用程序（包括数据库）的所有资源。图 18.14 给出了在这种情况下确保应用程序可用性

的解决方案。

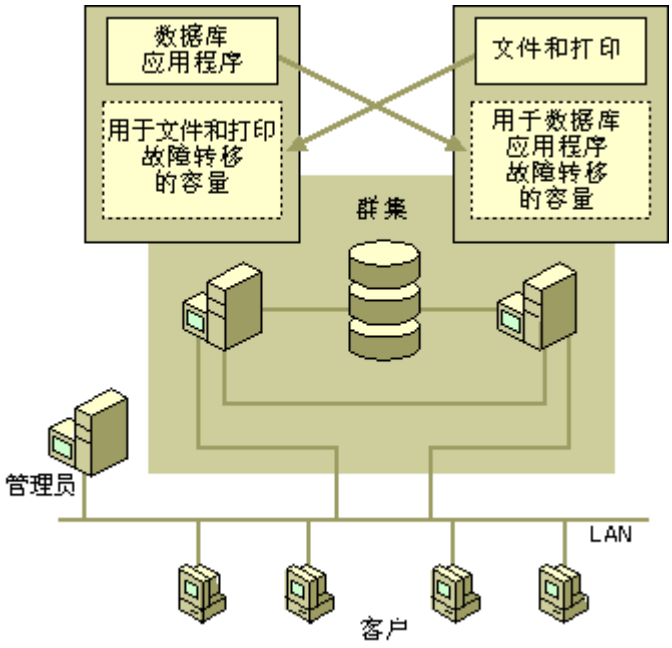


图 18.14 多个应用程序的群集

在每个组的故障转移策略中，请指定两个组都可以在任一节点上运行，从而保证其中一个节点发生故障时，两个组仍有可用性。

在 Windows 2000 Advanced Server 中，群集服务会检测服务器和客户系统之间连接的丢失。如果群集服务软件可以将问题隔离在特定的服务器，群集服务将宣布网络故障并将非独立组故障转移到另外一台服务器（通过工作的网络）。

部署示例 3:复杂混合配置

复杂混合配置是其它模型的混合。混合配置让您能将以前模型并为一个群集从而合并其优点。只要提供足够的容量，许多类型的故障转移方案可以在所有节点上共存。所有故障转移活动都根据设置的策略象平常那样发生。图 18.15 给出了多个数据库共享的一个例子，当共享在单一节点上时，允许性能有一定程度的降低。

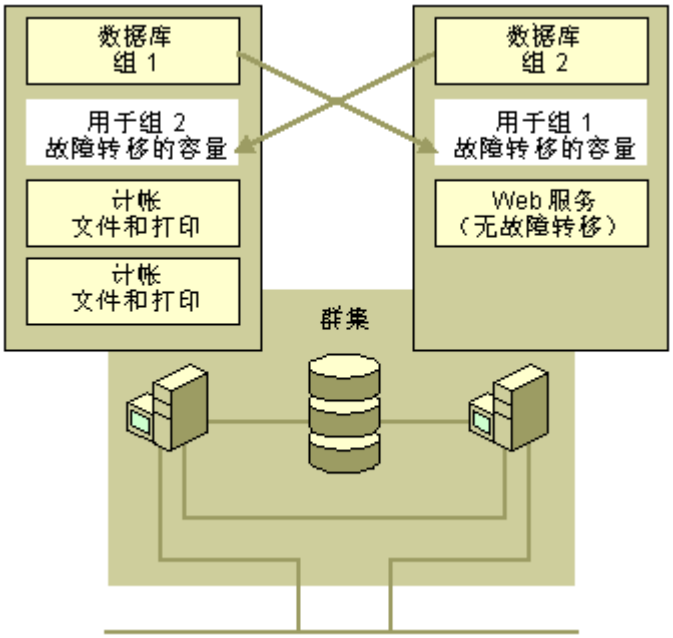


图 18.15 复杂混合配置

为了方便管理，群集（不要求故障转移能力的）中的文件和打印共享在逻辑上按部门分组并配置为虚拟服务器。最后，不能故障转移的应用程序驻留在其中一个群集上，并正常运行（没有任何故障转移保护）。

规划群集服务

在评估了群集需求之后，便可以开始确定需要多少服务器以及用什么规格，如多少内存和硬盘存储空间。

规划资源组

因为组中的所有资源都作为一个单元在节点间移动，非独立资源将不会超出单一组的界限（资源不能依赖其它组的资源）。

图 18.16 显示了非独立资源如何组合成组。右边的节点包含 Web 服务器组，它包括 IIS 依赖的四个资源：网络名称、IP 地址、IIS 虚拟服务和磁盘 E。

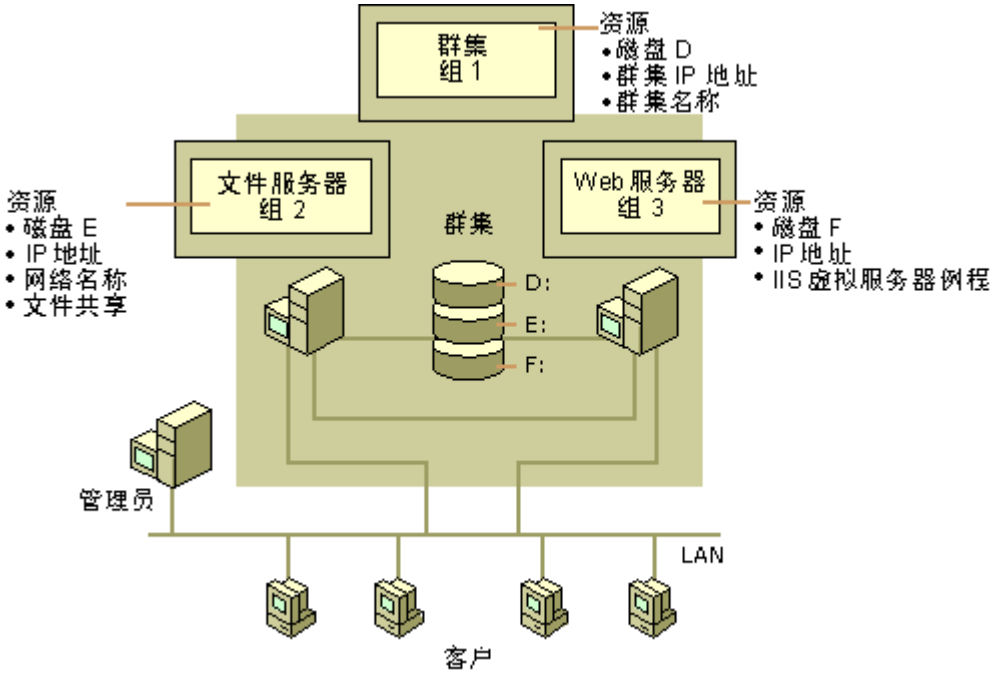


图 18.16 非独立资源的组

典型的群集为群集上运行的每个独立应用程序或服务提供一个组。典型的群集组包含以下类型的资源：

- IP 地址
- 网络名称
- 物理磁盘
- 普通或自定义应用程序或服务

将应用程序和其它资源组织为不同的组有六个步骤：

1. 列出基于服务器的所有应用程序。

   大多数组包含一个或更多应用程序。请制定环境中所有应用程序的列表，不管其是否计划用于群集服务。将计划在环境中运行的组（虚拟服务器）的总数与计划与组分开运行的软件的总数相加，从而确定出总容量要求。

2. 确定哪些应用程序可以使用故障转移。

   同时请列出将驻留在群集节点，但却因为不方便、没有必要、或不可能配置故障转移从而不使用故障转移功能的应用程序。虽然不为这些应用程序设置故障转移策略或将它们安排进组，它们仍会使用一部分服务器容量。

   在应用程序加入群集之前，请检查应用程序许可证，或与应用程序供应商核实。每个应用程序供应商都为在群集中运行的应用程序设置了不同的授权策略。

3. 列出所有非应用程序资源。

   请确定在您的网络环境中，服务器群集可以保护哪些硬件、连接和操作系统软件。

例如，群集服务可以将打印后台处理程序故障转移，以保护客户对打印服务的访问。另一个例子是文件服务器资源，可以将它设置为故障转移从而保持客户对文件的访问。这两种情况，容量都受到影响，如当发生故障转移时需要 RAM 为客户服务。

4. 列出每项资源的所有依赖关系。

群集服务维护着一个资源依赖关系的层次结构，以保证特定应用程序依赖的所有资源在应用程序之前已经联机。它还会保证应用程序及其依赖的所有资源在这些资源中的一项发生故障时，要么重新启动，要么故障转移到其它节点。

请创建依赖关系列表，以帮助确定资源和资源组彼此的相互依赖关系，以及资源在所有组之间的最佳分布。在其中请加入支持核心资源的所有资源。例如，如果 Web 服务器应用程序故障转移，Web 地址和共享总线上包含该应用程序文件的磁盘也必须故障转移（如果 Web 服务器要工作的话）。所有这些资源必须属于同一组。这保证了群集服务使相互依赖的资源始终在一起。

备注 在将资源分组时，请记住资源及与其有依赖关系的资源必须同处一组，因为资源不能跨越几个组。

资源组是故障转移的基本单位。单个资源不能独立地故障转移。资源将和同一资源组中的其它所有资源一起故障转移。

因为大多数应用程序将应用程序数据存储在磁盘上，所以建议为每个磁盘都创建资源组。将应用程序与其依赖的所有其它资源一起放入包含磁盘的组中，应用程序将在磁盘上存储数据。将其它应用程序及其磁盘放入其它组中。这一配置允许应用程序独立地故障转移或移动，而不会影响其它应用程序。

5. 制定初步的分组决定。

将应用程序分配在一组中的另一原因是为方便管理。例如，如果将特定的应用程序视为一个整体，会使网络管理起来更容易，那么可以将这几个应用程序放进一个组。

这种技术常见的应用是，把文件共享资源和打印后台处理资源并入一个组。如果将这些资源合并，所有与应用程序有依赖关系的资源也必须也在同一组中。您可以给这个组取一个能够代表其单位部门的唯一名称，如 AccountingFile&Print。每当需要干预该部门的文件共享和打印共享活动，就可以在群集管理器中寻找该组。

另一个常见做法是，将依赖特殊资源的多个应用程序放入同一组中。例如，假定 Web 服务器应用程序提供了对 Web 页的访问，而那些 Web 页提供一些结果，客户可通过查询 SQL 数据库应用程序访问这些结果。(查询通过使用超文本标记语言 [HTML] 格式进行)。通过将 Web 服务器和 SQL 数据库放在同一组，两个核心应用程序的数据都可以驻留在特定的磁盘卷上。因为两个应用程序共存于同一组中，您还可以专门为这个资源组创建 IP 地址和网络名称。

6. 制定最后的分组任务。

在将资源分组之后，给每个组取不同的名称，并创建依赖关系树。依赖关系树对于将资源之间的依赖关系形象化表示很有用。

要创建依赖关系树，请记录下组中的所有资源。然后对每个资源，将其与该资源直接依赖的其它每个资源用箭头连接起来。

例如，资源 A 和资源 B 之间的直接依赖关系意味着在两者之间没有中介资源。当在资源之间存在传递关系时，它们之间关系是间接依赖关系。如果资源 A 依赖资源 B，而资源 B 依赖资源 C，那么资源 A 和资源 C 之间存在间接依赖关系。但资源 A 不直接依赖资源 C。

图 18.16 中的 Web 服务器组中，网络名称资源和 IIS 虚拟服务器例程资源都依赖于 IP 地址资源。但在网络名称资源和 IIS 虚拟服务器例程资源之间没有依赖关系。

图 18.17 图示的一个简单的依赖关系树中，显示了最后的分组任务中的一些资源。

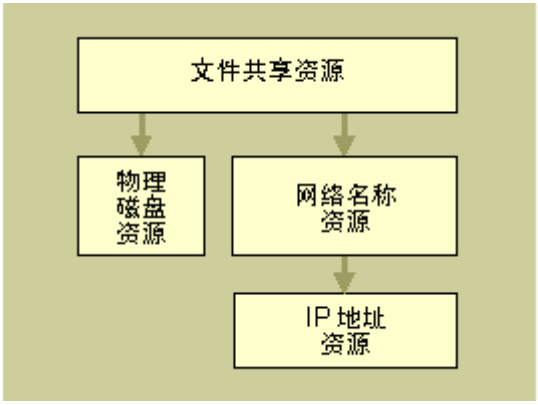


图 18.17 一个简单的依赖关系树

图 18.17 中，文件共享资源依赖网络名称资源，而网络名称资源又依赖于 IP 地址资源。但文件共享资源不直接依赖 IP 地址资源。

备注 物理磁盘不会依赖其它任何资源，并可以独立地故障转移。

确定群集服务的容量要求

如果已经完成了以下任务，便可以开始为群集中的每台服务器确定硬件容量要求了。

- 选择了群集模型。
- 确定了如何将资源分组。
- 确定了每个资源要求的故障转移策略。

以下几段中提出了一些标准，可以帮助您为用作群集节点的计算机确定硬件要求。

硬盘存储要求 群集中的每个节点必须有足够的硬盘容量，以存储运行所有组所要求的所有应用程序的永久副本及其它资源。在计算每个节点的硬盘存储空间时，要假定群集中所有这些资源都在该节点上运行，即使组中的一些或全部资源大部分时间都在其它节点上运行。为磁盘空间留出余量，可以在故障转移时让任何其它节点能够高效运行所有资源。

备注 群集服务不支持动态磁盘及逻辑卷管理器提供的新功能。特别是，群集服务管理的磁盘 NTFS 文件系统分区不能被扩展。您需要规划磁盘容量，并为预期增长留出足够的空间。

CPU 要求 故障转移在一个节点控制故障节点的资源时，会使该节点的 CPU 处理容量显得紧张。若没有适当的规划，在故障转移时，幸存节点的 CPU 的工作负荷将可能超过其实际能力，从而使响应用户的时间减慢。请规划每个节点的 CPU 容量，以使其适应新增资源，而不会影响响应时间。

RAM 要求 在规划容量时，要确保群集中的每个节点都有足够 RAM 来运行可能在任何其它节点上运行的所有应用程序。同时，要确信已为每个节点定义的 RAM 量正确设置了 Windows 2000 Advanced Server 页面文件。

服务器群集的限制

Windows 2000 Server 群集的一些重要限制如下。

可移动存储

- 请不要在群集中 SCSI 共享总线上安装可移动存储设备。
- 不要将可移动存储设备（如磁带更换器）配置为群集资源。

磁盘配置

- 必须使用 NTFS 文件系统格式化群集存储中的磁盘，并将其配置为基本磁盘。但 NTFS 不支持在群集存储中使用动态磁盘。
- 在群集存储中，不能使用加密文件系统、远程存储、固定卷或重剖析点。

不能在内部 RAID 控制器中启用写缓存，因为缓存中的数据在故障转移时会丢失。一个内部控制器的例子是节点内的外设部件互连 (PCI) 卡。视 RAID 控制器的不同，您可以在一个外部 RAID 控制器上启用写缓存。外部 RAID 控制器通常放在磁盘柜中，缓存中的数据可以故障转移。

- 只能在本地驱动器上使用软件 RAID （即，不由群集服务管理的驱动器）。只能使用硬件 RAID 来保护群集磁盘上的数据。

网络配置

- 群集服务只支持 TCP/IP。
- 服务器群集中，所有节点使用的所有网络接口必须在同一网络上。所有群集节点必须至少有一个公共子网。
- 终端服务

可以在服务器群集节点中使用终端服务进行远程管理。但不能在服务器群集节点中将终端服务用于应用程序服务器。

重要提示 目前，您还不能在同一服务器中使用网络负载平衡和群集服务。

自动部署群集服务的工具

有一些工具可以让企业中的部署群集服务自动化。在 Windows 2000 产品光盘 (CD) 中提供了这些工具。表 18.2 对它们做了说明。

表 18.2 自动部署群集服务的工具

工具	说明
Sysprep	启用磁盘复制的工具。可以将 Windows 2000 Advanced Server 操作系统和应用程序装在一台计算机上，然后把该安装复制到任意多个系统。
Cluscfg.exe	此工具包括在基本操作系统中。任何时候在系统中安装群集服务，都需要运行该工具以配置群集。

Setup Manager	一种基于向导的工具，它可帮助为定期的无人参与和 Sysprep 部署创建无人参与脚本和网络分发共享。

以下示例说明了如何使用这些工具。

如果要部署群集服务的系统硬件配置完全不同，您可以使用无人参与安装程序来安装这些系统。这包括创建一个 Unattend.txt 文件和网络分发共享（可选），以自动化安装程序（包括配置 Windows 2000 群集服务）。

如果硬件配置类似，可以使用 Sysprep 创建映像，以加快安装和部署过程。要使用 Sysprep 部署 Windows 2000 群集服务，必须首先安装该群集服务（在“Windows 组件向导”中选择它）。在系统中部署完映像后，您可以运行 Cluscfg.exe 文件。可以通过将 Cluscfg.exe 放在 Sysprep 应答文件的 [GuiRunOnce] 段，使运行 Cluscfg.exe 自动进行。这样，在 Sysprep 完成运行之后，Cluscfg.exe 在每个系统上运行。您可以使用应答文件使执行 Cluscfg.exe 自动化。

有关这些工具的更多信息，请参见 *Distributed Systems Guide* 中的“Windows Clustering”。

优化群集

Windows 2000 Advanced Server 使用了自适应体系结构，当遇到性能问题时它在很大程度上可以自我调整。另外，Advanced Server 能够按需要动态分配资源以适应变化的使用要求。

调整服务器及其平衡负载的应用程序，目标是确定对哪些硬件资源的需求最强，然后调整配置以满足这种需求，使总的吞吐量达到最大。

例如，如果群集的主要任务是提供文件和打印服务的高可用性，由于大量的文件被访问会导致磁盘使用率很高。文件和打印服务同时还会由于移动大量的数据，造成网卡负载加重。确保网卡和群集子网能够处理这些负载非常重要。在本例中，RAM 通常并不承担很重的负载，尽管在大量的 RAM 被分配到文件系统缓存时，内存使用也很严重。这种环境下，处理器使用率通常也很低。在这种情况，内存和处理器的使用通常不需要象其它组件那样进行优化。内存常常可以有效地使用以降低磁盘的使用，特别是在磁盘读取操作时更是如此。

相反，服务器应用程序环境（如 Microsoft Exchange）比一般的文件或打印服务器环境更消耗处理器和 RAM，因为在前者的服务器上需要更多的处理。在这种情况下，最好是使用高档的多处理器服务器。磁盘和网络负载往往较少使用，因为传送的数据量较少。Microsoft 负载平衡解决方案中，用于主机到主机的通信或群集本身运行的系统资源很少。

规划容错磁盘

磁盘故障可能导致重要数据丢失，无法挽回，并导致负载平衡服务与服务器及所有其它应用程序停止工作。有鉴于此，不妨考虑使用特殊方法保护磁盘，防止发生故障。

很多资源组包括共享总线上的磁盘资源。某些情况，它们是简单物理磁盘，但在其它情况下它们却是包含多个磁盘的复杂磁盘子系统。几乎所有资源组都依赖共享总线上的磁盘。磁盘资源不可恢复的故障会导致包含这些资源的组出现某些故障。鉴于这些理由，您可能决定使用特殊的方法来保护磁盘和磁盘子系统，防止发生故障。

一个常见的解决方案是使用基于硬件的 RAID 解决方案。RAID 能确保群集磁盘组中包含的数据有高可用性。一些基于硬件的解决方案被认为是容错的，这意味着如果磁盘组的一个成员发生故障，数据不会丢失。

硬件 RAID

Microsoft Windows 2000 HCL 包含了许多不同的用于群集的硬件 RAID 配置。许多硬件 RAID 解决方案在一个机柜内提供电源冗余、总线冗余和电缆冗余，并可以跟踪硬件 RAID 固件中每个组件的状态。这些能力的意义在于，它们用多个冗余提供了数据的可用性，防止多个点发生故障。硬件 RAID 解决方案还可以使用板上处理器和缓存。

Windows 2000 Advanced Server 可以使用这些磁盘作为标准磁盘资源。

尽管比软件 RAID （作为 Windows 2000 Advanced Server 提供的一种功能包括）昂贵许多，硬件 RAID 通常还是被认为是上好的解决方案。

错误恢复

运行任何 Windows 2000 Advanced Server 负载平衡服务的计算机都象其它计算机一样，受到故障风险威胁。计算机发生故障的原因多种多样，只要可能，建议您始终采取适当的防范措施防止潜在的故障点发生故障。这些防范措施包括，软件和硬件 RAID、不间断电源、事务日志和恢复（这是 NTFS 文件系统的一项功能）。为了使用这些功能，请务必将负载平衡服务放在以 NTFS 格式化的分区上。

通过事务日志和恢复，NTFS 会保证卷结构不会被破坏，因此在系统发生故障后，所有文件仍可以使用。NTFS 同时还使用了称为“ 群集重映射 ”的恢复技术。当 Windows 2000 Advanced Server 向 NTFS 报告坏扇区错误时，NTFS 会动态地替换包含坏扇区的磁盘群集，并给数据分配新的磁盘群集。如果错误发生在读取阶段时，NTFS 给调用程序返回读取错误，而数据丢失（除非它由 RAID 容错保护）。如果错误发生在写阶段，NTFS 会将数据写到新的磁盘群集，没有数据丢失。NTFS 将包含坏扇区的磁盘群集的地址放入其“ 坏扇区 ”文件，以使它不再使用坏扇区。

如果不使用容错磁盘解决方案，即使有事务日志和恢复及磁盘群集重映射，您也可能因为硬件故障丢失用户数据。

测试服务器容量

在使单位的应用程序和服务具有高可用性时，测试服务器的容量以避免服务器故障也相当重要。

以下列表给出了需要测试的一些硬件组件：

- 独立的计算机组件，如硬盘和控制器、处理器和 RAM。
- 外部组件，如路由器、网桥、交换机、电缆和连线器。

下面是需要重点测试的一些项目：

- 繁重的网络负荷。
- 同一磁盘的繁重磁盘 I/O。
- 文件，打印和应用服务器的繁重使用。
- 同时进行大量登录。

Windows DNA Performance Kit （ Windows DNA 性能工具包）让您能测试和调整应用程序的性能。该工具包允许调整 Windows NT 4.0 Microsoft Transaction Server (MTS)、COM+、IIS 和 SQL Server 中的应用

程序，以提高组件负载平衡性能。

该工具包还包含了 COM+ 和 IIS 的性能信息及可以模拟许多用户同时访问 IIS 或 COM+ 应用程序造成的影响的工具。模拟许多用户是了解应用程序的硬件要求中很重要的一步。

备注 Windows DNA 性能工具包是为 Windows 2000 Advanced Server 或带 Windows NT Option Pack 的 Windows NT Server 4.0 设计的。

有关 Windows DNA 性能工具包及如何下载该工具包的更多信息，请参见 Web 资源页的“ Windows DNA Performance Kit ”链接，地址是 http://windows.microsoft.com/windows2000/reskit/webresources .

有关制定测试规划的更多信息，请参见本书的“ 建立 Windows 2000 测试实验室 ”。

规划群集备份和恢复策略

一个完整的群集备份包括：

- 群集配置的记录，包括哪些资源注册表项映射哪些资源。建议您这样做，因为每个资源注册表项都只用资源的全球唯一标识符 (GUID) 标识。
- 备份的编录。
- 备份到安全位置
- 若有必要，为每个节点制作紧急修复磁盘，以便恢复该节点的 Windows 2000 Advanced Server。

  紧急修复磁盘是使用“ 备份 ”制作的磁盘，包含了当前的 Windows 系统设置信息。如果计算机不能启动或系统文件被损坏或删除，可用该磁盘修复计算机。

  有关制作紧急修复磁盘的更多信息，请参见“ Windows 2000 Advanced Server 帮助 ”。

备份建议要求满足下列条件：

- 已制定并记录了恢复步骤。
- 已用功能完全相同的硬件（经 HCL 认可）更换了所有物理损坏的群集，所有群集磁盘都具有相同或更大的容量。

一个完备的备份规划应解决下列问题：

- 同步备份
- 创建备份存储空间
- 存储备份媒体
- 维护备份编录

有关备份和恢复例程和群集工具的更多信息，请参见 *Distributed Systems Guide* 中的“ Windows Clustering ”。

Windows 2000 群集规划任务列表

表 18.3 中的 Windows 2000 群集规划任务列表是有关本章讲述的重要任务信息的索引列表，您可以用它来帮助制定单位的应用程序和服务可用性策略。

表 18.3　Windows 2000 群集规划任务列表

任务	章节中的位置
组建群集规划小组	确定可用性策略
明确应用程序和服务的特定的高可用性需求。	确定可用性策略
确定群集要求。	确定可用性策略
确定哪些应用程序应用网络负载平衡。	规划网络负载平衡
使用网络负载平衡部署终端服务器群集。	规划网络负载平衡
为运行 IIS/ASP 和 COM+ 应用程序的服务器配置网络负载平衡群集。	规划网络负载平衡
识别网络风险。	规划网络负载平衡
进行网络负载平衡容量规划。	规划网络负载平衡
确定服务器容量要求。	规划网络负载平衡
优化网络负载平衡群集。	规划网络负载平衡
选择运行在服务器群集上的应用程序。	规划群集服务
识别网络风险。	规划群集服务
确定资源组的故障转移和故障回复策略。	规划群集服务
选择服务器角色。	规划群集服务
选择群集模型。	规划群集服务
进行群集服务容量规划。	规划群集服务
选择帮助您自动部署群集服务的工具。	规划群集服务
优化群集。	优化群集

规划容错磁盘。	规划容错磁盘
测试服务器容量。	测试服务器容量
规划备份和恢复策略。	规划群集备份和恢复策略

其它资源

- 有关 Windows 群集的更多信息，请参见“Windows 2000 Advanced Server 帮助”。
- 有关 Windows 群集 API 的更多信息，请参见 Web 资源页的“Microsoft Platform SDK”链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources .
- 有关 WinDNA 性能工具包的更多信息，请参见 Web 资源页的“WinDNA Performance Kit”链接，地址是： http://windows.microsoft.com/windows2000/reskit/webresources .

  有关各种硬件 RAID 配置的更多信息，请参见：

  - Web 资源页的“Microsoft Windows Hardware Compatibility List”链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources .
  - Web 资源页的“Microsoft TechNet”链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources .

第 19 章 - 确定 Windows 2000 存储管理策略

管理日常网络运行和了解数据管理和存储系统要求的网络管理员应该熟悉与 Microsoft® Windows® 2000 Server 存储管理相关的功能。

当规划 Windows 2000 的部署时，最好把这些新功能包括在存储管理策略中。磁盘管理，可移动存储，远程存储，Windows 群集，分布式文件系统，Microsoft® 索引服务以及其它功能可以帮助您改善存储管理活动。

本章还讨论选择数据存储系统、容错和备份策略的注意事项，以及提高灾难恢复能力的方法。

本章内容

提高存储管理能力
管理磁盘资源
优化数据管理
加强数据保护
提高灾难恢复能力
存储管理规划任务列表

本章目标

本章将帮助您创建以下规划文档：

- 存储配置策略
- 灾难恢复计划
- 存储管理计划

资源工具包中的相关信息

- 有关使用可移动存储和远程存储的详细信息，参见《 Microsoft® Windows® 2000 Server Resource Kit Server Operations Guide 》中的“Data Storage and Management”。
- 有关备份的规划，策略和措施的详细信息，参见《Server Operation Guide》中的“Planning a Reliable Configuration”。
- 有关灾难恢复的详细信息，参见《Server Operation Guide》中的“Repair, Recovery, and Restore”。

提高存储管理能力

改善存储系统及其管理不仅是部署 Microsoft windows 2000 Server 的重要考虑因素，而且是任何企业网络基础结构的关键组成部分。由于企业环境中存在着大量需保护的数据，必须了解最新的技术从而选择满足网络需要的最佳硬件和软件。

Microsoft Windows 2000 提供几种功能来管理磁盘资源从而提高性能并保护数据。这些功能包括下列部分：

磁盘管理 用于设置和组织磁盘存储系统。

可移动存储 用于管理新型的存储设备。

远程存储 用于把不用的文件转移到远程存储。

Windows 2000 下列功能帮助您更有效地管理数据：

Windows 群集 用于使管理更简便并使数据及应用程序可用性更高。

文件系统改进 用于提高包括 NTFS 文件系统和配额管理在内的共享的信息和资源的性能，可用性，安全和可管理性。

分布式文件系统 (Dfs) 用于把共享资源连成单一的名称空间，使查找和管理数据更简易。

索引服务 用于基于内容和属性的快速文件搜索。

除了这些功能之外，Windows 2000 还提供容错和备份功能来帮助您加强数据的保护。

下面的部分将更详细地讨论这些功能。除了熟悉 Windows 2000 的存储管理功能之外，您应当在部署规划文档中包括存储管理规划。

制定存储管理规划

制定存储管理规划时需要考虑许多问题。企业级的单位应该考虑成立一个存储管理小组来确定数据存储需要并创建有关的计划。一些单位有可能发现本章中讨论的问题最好由许多不同的小组来处理，例如备份和灾难恢复小组，数据管理小组以及处理存储问题的小组。每个小组从评估单位的存储需要和制定存储管理策略开始。

为了帮助您制定存储管理规划，考虑使用图 19.1 所示的步骤。

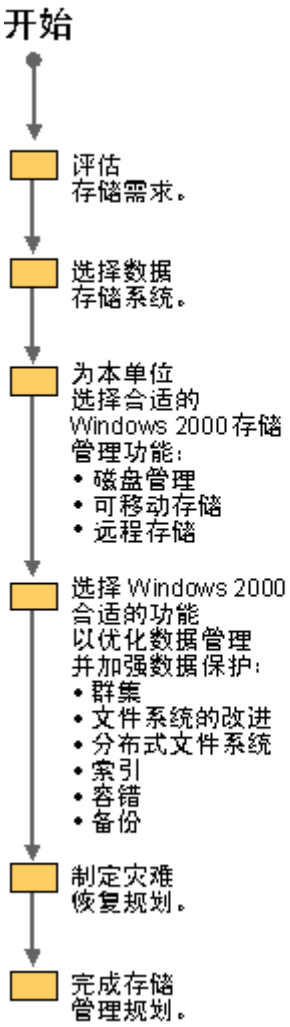


图 19.1 制定存储管理策略的过程

评估存储需求

随着企业网络的数量及大小的扩大，网络存储解决方案也迅速地不断涌现。每一个单位在选择数据存储的媒体和方式时有不同的优先考虑。一些单位为费用所制约，另一些则把性能置于其它考虑之上。

当评估存储需要时，您需要考虑可能的数据、效率和业务的损失与提供高性能和高可靠性的存储系统的花费之间取舍。制定存储管理策略之前考虑下列需要：

- 对您所在单位性能价格比最合适的技术。
- 可以随网络的扩大而扩展的合适存储容量。
- 快速，24 小时访问关键数据的需要。
- 适合数据存储需要的安全的环境。

当挑选性能价格比最好的解决方案时，必须在购买和维护软件和硬件的开销与灾难性的数据丢失的后果之间权衡利弊。开销包括：

- 最初的硬件投资，例如磁带和磁盘驱动器，电源，以及控制器。
- 相关的媒体，例如磁带和光盘。
- 软件，例如存储管理工具和备份工具。
- 日常硬件和软件维护开销。
- 人员工资。
- 使用新技术的培训。
- 站外存储设备。

把这些开销与如下费用相比较：

- 文件服务器，邮件服务器或打印服务器的更换费用。
- 更换运行应用程序（例如 Microsoft® SQL Server™ 或 Microsoft® Systems Management Server (SMS)）服务器的费用。
- 更换运行路由和远程访问服务、Microsoft® SNA Server、Microsoft Proxy Server 或 Novell NetWare 的网关服务器的费用。
- 为不同部门的人员更换工作站的费用。
- 更换单独计算机组件（例如硬盘或网卡）的费用。

选择存储系统时需要考虑的另一个重要的因素是数据恢复的速度。如果一个服务器上的数据丢失了，您能多快地恢复那些数据？您能够容许一个服务器（或者整个网络）瘫痪多长时间而不严重地影响业务的运转？

存储技术发展地非常迅速，所以在您作出购买决定前最好研究每一类型的相对优势。您使用的存储系统应该有足够的容量备份最关键的数据。它还应该在备份和恢复操作中提供错误检测和纠正。

选择数据存储系统

回答下列问题来确定最能满足您需要的存储系统：

现在您需要存储多少数据？

如果必须存储非常多的数据，基于磁带的存储系统也许是您最好的选择。磁带的每兆字节媒体成本大大低于其它类型的存储媒体。

您预期的数据存储需求是怎样的？

许多单位的存储需求每年倍增。考虑购买比满足现有需要更大的存储系统或能够随需求增长而扩展的可伸缩系统。为了评估这一点怎样影响情况，将几年前的数据存储与您现在的水平对比，并使用这一增长率估计您未来的需要。

多少用户或应用程序同时访问数据存储系统？

许多供应商提供允许同时访问几个驱动器的多驱动器系统。这样，多个用户或应用程序可以同时访问系统而不会影响性能。

数据访问时间有多重要？

如果资料库主要用于实时数据访问，那么这是您最重要的问题。如果数据访问时间是您首要的考虑，基于 CD-ROM 的方案工作得最好，因为 CD-ROM 的随机存取能力把查找时间减到了最短。数据访问时间包括两个部分：查找时间和传送速率。这一方案的不足之处在于速度和费用：除非使用高速驱动器，数据传送速率低于基于磁带的系统；而且每兆字节费用高于磁带媒体。

数据传送速率有多重要？

如果数据存储系统主要用于存档和备份数据，那么数据传送速率是您最重要的问题。如果是这样的情况，基于磁带的解决方案最好，因为磁带驱动器的数据传送速率是 CD-ROM 驱动器的十倍。而且基于磁带系统的每兆字节费用也较低。磁带的不足之处在于线性文件访问使文件访问时间增加了若干倍。

预算有多大？

再者，在决定可以支付多少费用之前，将不稳定的硬件造成的数据丢失或毁坏和故障时间带来的潜在费用考虑在内。如果存储的数据对您所在单位非常重要，这些风险就使得购买廉价方案带来的费用节省得不偿失。

而且，要考虑总体费用。一些硬件购买时相对便宜但是每兆字节费用却相当昂贵。基于 CD-ROM 的系统就是这样。更常见是，在一段时间之后用于媒体的费用高于用于最初的硬件费用。

为帮助您选择存储系统，尝试创建两个或更多模型，上面采用具有不同存储容量和数据保护等级的硬件和软件方案。记住要考虑预期的增长。

表 19.1 列出了可能的硬件和软件解决方案的相对能力：5 表示可用的最好方案；1 表示最不理想的方案。使用该表来为单位选择存储类型。

表 19.1 供选择的硬件和软件存储方案

方案	可用性	响应时间	容量	多用户支持
CD-ROM/DVD-ROM	4 [1]	3	2-3	2
CD-ROM 库	4	2	5	5
CD-ROM 驱动器阵列	5	4	4	4
Dfs	5	3-4	5	5
磁盘	3	4	3	3
双控制器磁盘镜像（双工）	5	4	2-3	2
磁盘带区集	1	5	4	4
带有奇偶校验的磁盘带区集	4	3	3-4	4
磁带	3	2	4	1
磁带库	3	1	5	4

[1] 5 – 高 /1 – 低

当您组成存储管理队伍，明确存储需求并且决定了预算之后，您需要评估 Windows 2000 的存储能力。

管理磁盘资源

Windows 2000 提供了几项存储功能来帮助您存储和管理数据，包括磁盘管理，可移动存储和远程存储。接下来的部分将介绍这些功能。

磁盘管理

Microsoft 管理控制台 (MMC) 的磁盘管理管理单元是管理磁盘存储系统的一个工具。向导会引导您创建分区或卷并且初始化或将磁盘升级。Windows 2000 Server 磁盘管理新的关键功能包括：

联机磁盘管理 在不用关闭系统或干扰用户的情况下完成绝大多数管理任务。例如，可以不用重新启动系统而创建各种的分区布局并选择保护策略，如镜像和带区。不用重新启动而新增驱动器。大多数配置更改立即生效。

远程磁盘管理 作为管理员，可以管理任何运行 Windows 2000 的远程（或本地）计算机。

图 19.2 是您在磁盘管理中可以选择一些“ 视图 ”菜单选项

图 19.2 磁盘管理 MMC 管理单元

基本和动态存储

Windows 2000 有两种可用的磁盘存储方式：基本或动态。基本存储支持面向分区的磁盘。基本磁盘可以包括主磁盘分区，扩展磁盘分区和逻辑驱动器。基本磁盘还可以包括跨区卷（卷集）、镜像卷（镜像集）、带区卷（带区集）和冗余独立磁盘阵列或 RAID-5 卷。在 Microsoft® Windows® version 4.0 或更早版本，RAID-5 也称为带有奇偶校验的带区集。如果您希望计算机访问这些卷并且这些计算机运行 Windows NT 4.0 或更早版本，Microsoft® Windows® 98 或更早版本，或 Microsoft® MS-DOS，您需要创建基本卷。

动态存储支持新的面向卷的磁盘，这是 Windows 2000 的新功能。它克服了面向分区磁盘的组织限制并有助于多磁盘，容错磁盘系统的运行。使用动态存储，不用重新启动操作系统就可以进行磁盘和卷管理。在动态磁盘上，存储区被划分为卷而不是分区。一个卷包括下列布局中的一个或多个物理磁盘的一部分或几部分：简单卷、跨区卷、镜象卷、带区卷和 RAID-5 卷。动态卷不能包括分区或逻辑驱动器，而且不能被 MS-DOS 或 Microsoft® Windows® 98 和更早版本访问。可以使用动态存储及多个磁盘组成一个容错系统。

当向计算机增加新的磁盘时，创建卷或分区前应该初始化该磁盘。初始化磁盘时，如果您希望在磁盘上创建简单卷或者希望共享该磁盘从而和其它磁盘共同创建跨区卷、带区卷、镜象卷和 RAID-5 卷时，请选择动态存储。如果希望在磁盘上创建分区和逻辑驱动器，选择基本存储。

表 19.2 列出了使用磁盘管理以基本和动态磁盘可以执行的任务。

表 19.2 用基本和动态磁盘可执行的任务

任务	基本磁盘	动态磁盘
创建和删除主磁盘分区和扩展磁盘分区。	X	
在扩展磁盘分区中创建和删除逻辑驱动器。	X	
格式化和标记分区并将其标记为活动。	X	
删除卷集。	X	
从镜像集中分离出一个镜像。	X	
修复镜像集。	X	
修复带有奇偶校验的带区集。	X	
将基本磁盘升级为动态磁盘。	X	
创建和删除简单卷、跨区卷、带区卷、镜象卷和 RAID-5 卷。		X
将卷扩展到一个或多个磁盘上。		X
添加镜像或从镜像卷删除镜像。		X
修复镜像卷。		X
修复 RAID-5 卷。		X

检查有关磁盘的信息，例如容量，可用空间和当前状态。	X	X
查看卷和分区的属性（例如大小）。	X	X
分配和更改硬盘卷以及分区和 CD-ROM 设备的驱动器名。	X	X
创建卷的装入点。	X	X
设置或验证卷或分区的磁盘共享和访问设置。	X	X

卷管理

Windows 2000 包括对卷管理结构的显著改进。卷管理包括在系统中创建、删除、更改和维护存储卷的过程。新体系结构提高了企业环境中卷的可管理性和可恢复性。

该体系结构中增添了逻辑磁盘管理器 (LDM) 用来扩展容错功能，改善系统恢复，封装卷信息，从而使磁盘可以轻松地移动，管理功能得以改善。这一服务负责创建和删除卷，容错功能 (RAID) 和卷跟踪。使用磁盘管理单元管理本地和远程卷。

卷管理有如下功能：

- 在一个物理硬盘的可用空间上创建任意数目卷或创建跨越两个或更多磁盘的卷。
- 同一磁盘上的不同卷可以有不同的文件系统，例如文件分配表 (FAT) 文件系统或 NTFS 文件系统。
- 对磁盘的大多数更改立即可用。不需退出磁盘管理来保存或重新启动计算机来使用它们。

卷的装入点

作为磁盘管理的一部分，可以创建卷的装入点。卷的装入点提供了一种快速使数据联机和脱机的方法。它们是 Windows 2000 内部名称空间中代表存储卷的文件系统对象。当把卷的装入点放入一个空的 NTFS 目录时，不必指定额外的驱动器号就可以把新的卷移植到名称空间中。卷的装入点的一种使用方法是把一部有单一驱动器和卷的计算机格式化为 C 并且把该磁盘装载为 C:\Games。

卷的装入点的一些可能应用包括：

为应用程序提供额外的空间 例如，您把磁盘装载为 C:\Program Files。当需要额外的磁盘空间时，可以向系统添加磁盘并使其和位于 C:\Program Files 的磁盘跨接。

创建新的存储类型 例如创建一个带区集以提高性能并将其装载为 C:\Scratch；创建一个镜像集以保证稳定性并将其装载为 C:\Projects。用户可正常看到目录，但是他们的 scratch 目录会很快，而 projects 目录会得到镜像集的保护。

为卷创建多个装入点 例如，一个卷装载为 C:\Games 和 C:\Projects。要注意没有什么阻止名称空间中的循环。如果您把一个卷装载为 D 和 D:\Docs ，因为 D 装载在它自身之下，这样就在名称空间中创建了一个循环。做列举的应用程序会在这个卷上陷入死循环。

卷的装入点相对于计算机添加或删除硬件设备时发生的系统变更来说是稳定的。您能够创建的卷的数目不再

会被驱动器名的数目所限制。

磁盘碎片整理

磁盘管理的另一功能是磁盘碎片整理程序。可以使用这一工具找到已经变为碎片的文件和文件夹，并且重新组织本地磁盘卷上的簇。磁盘碎片整理程序整理簇使得文件、目录和可用空间在物理上更连续。结果是系统可以更有效地访问和存储文件和文件夹。如果碎片相当多，磁盘碎片整理程序可以相对于磁盘输入/输出 (I/O) 显著地提高整个系统的性能。

磁盘碎片整理功能决定文件储存在磁盘上的位置，但是 NTFS 和 FAT 将簇移来移去。

可以在格式化为 FAT16、FAT32 或 NTFS 的卷上使用该工具。

使用动态存储的注意事项

创建卷时考虑下列因素：

- 动态存储使用面向卷的方案组织磁盘。Windows NT Server 和动态磁盘不兼容。
- 可以在向 Windows 2000 Server 升级时使用 Windows 2000 安装程序来配置磁盘空间。

  备注 可以在磁盘未分配的部分创建新的卷和分区而不会丢失现有卷中的数据。但是如果您试图改变卷的拓扑，必须备份数据，因为对现有卷的改动会清除所有现存数据。

- 可以在最初安装和加载 Windows 2000 Server 操作系统软件时配置新计算机的内部硬盘。可以在安装之后使用磁盘管理对磁盘进行更改。

有关管理磁盘的详细信息，参见《Microsoft® Windows® 2000 Server Resource Kit Server Operations Guide》中的“Disk Concepts and Troubleshooting”。

可移动存储

可移动存储系统是一项新技术，它可使得多个应用程序可以共享本地库以及磁带或磁盘驱动器，这样存储管理功能得以改善。有了可移动存储，可以使用独立的存储设备；管理联机媒体库和自动变换器；跟踪可移动磁带和磁盘。独立设备包括 CD-ROM、DVD-ROM、磁带（4 毫米、DLT、8 毫米及其它），以及高容量磁盘驱动器。

可移动存储还控制单服务器系统中的可移动媒体。除此之外，它还和备份和远程存储一起执行功能。可移动存储的一个重要方面是应用程序能够创建其自身拥有和使用的媒体池。

存储设备通常使用小型计算机系统接口 (SCSI) 适配器或大多数硬盘使用的集成电路设备 (IDE) 接口连接到系统上。Fiber Channel ，IEEE 1394 和 Intelligent I/O (I20) 等简单易用并提供高吞吐量的新技术越来越频繁地得到应用。独立设备在单用户系统中使用得最为广泛。

媒体库由使用 CD-ROM、DVD-ROM、磁光 (MO) 盘或磁带的多个驱动器组成。这些与为管理单个媒体或存储提供广泛自动化的自动控制器一起使用。容量范围从小型的三碟 CD-ROM 自动换片机到大公司使用的与完善的应用程序一起使用的磁带或盘片媒体库。媒体库在服务器上使用得最多,但也越来越多地连接到单用户系统上。

使用可移动存储可以完成的任务包括：

- 跟踪联机和脱机媒体

- 装载和卸载媒体
- 在媒体库中插入和取出媒体
- 查看媒体和媒体库的状态
- 创建媒体池并设置媒体池的属性
- 为媒体和媒体池设置安全参数
- 创建媒体库清单

备注 备份软件必须和可移动存储兼容才能使用这些功能。

远程存储

远程存储是为 Windows 2000 Server 提供的一种分层存储管理系统。使用远程存储时，您使用远程存储 MMC 管理单元把不用的文件移到磁带库中去。定期迁移文件可以增加磁盘上的可用空间。从用户的角度看，迁移过的文件仍然是活动的，但访问时要花费更长的时间。

存储层次有两个级别。最高的一级叫做本地存储。它由在 Windows 2000 server 上运行远程存储的计算机上的本地 NTFS 卷组成。远程存储控制的本地磁盘卷叫做被管理卷。

叫做远程存储的较低一级存储级别存储从本地存储复制到联机媒体库或其它存储设备的数据。

当本地卷上的可用空间量降到您需要的水平之下时，远程存储从以前被复制到远程存储的本地文件中截去数据，这样就提供了更多可用磁盘空间。当数据被截去后，它留下文件标记以使您能访问那个文件。远程存储依照管理员为每一本地存储卷设定的原则管理数据的移动。可以设定从某一特定卷移动文件备份日程安排，还可以设定需要移动的文件的标准和规则。更确切的说，可以：

- 分配和配置远程存储设备和媒体。
- 设置系统范围内的远程存储功能选项。
- 为远程存储管理的卷配置卷管理设置。
- 查看远程存储活动信息。
- 从媒体灾难中恢复。
- 创建和提交作业。

因为媒体库中的可移动磁带的每兆字节费用比硬盘更便宜，因而这是提供最大数据存储和最优本地磁盘性能的经济方式。

备注 备份和病毒扫描软件必须和远程存储兼容。管理员必须保证激活远程存储前进行卷范围内的操作，这样就不必把所有的东西都移回磁盘上。备份从磁带上直接读取数据。

远程存储和可移动存储之间的关系

远程存储使用可移动存储把数据复制到包含可移动媒体的联机媒体库。图 19.3 是这些存储系统和各种存储设备之间关系简图。

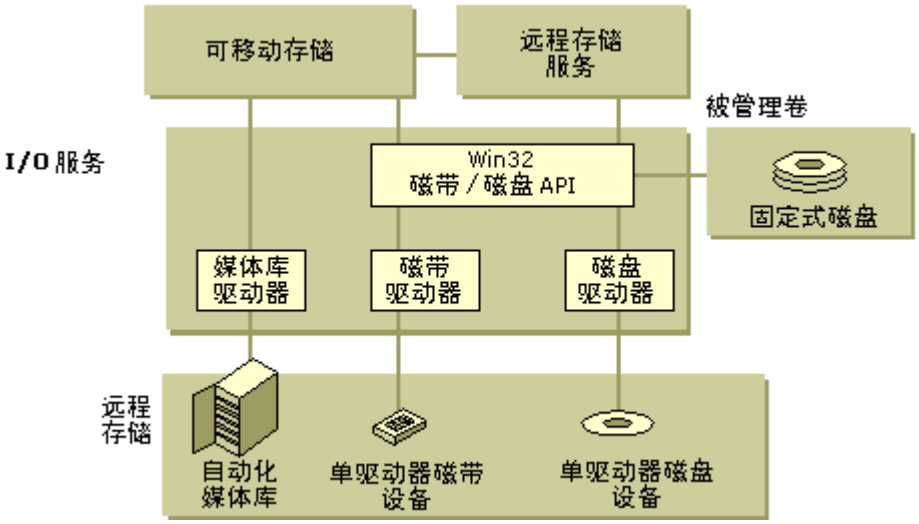


图 19.3 远程存储、可移动存储和存储设备之间的关系

使用远程存储的注意事项

使用远程存储具有下列优点：

- 使用低成本的远程存储使本地存储空间虚拟扩充。
- 对远程存储中对数据透明自动访问。
- 与日常手工数据管理操作相关的劳动密集的操作自动执行。
- 多个卷的远程存储的集中共享。

远程存储不是备份的替代方案，因为只有数据的一个实例存在。有规律地备份卷是至关重要的。备份和远程存储集成在一起，从而不必把所有的东西都移回磁盘上；备份从磁带上直接读取数据。

优化数据管理

能够帮助您在企业环境中有效地管理数据的 Windows 2000 功能包括：

- Windows 群集
- NTFS 文件系统
- 配额管理
- 分布式文件系统 (Dfs)
- 索引服务

Windows 群集

当您需要更高的可用性和简便的管理时，考虑在企业网络存储策略中使用群集。群集提供在单一服务器故障时维持系统运行的体系结构，从而减少故障时间。

使用 Windows 群集，可以连接两个或多个服务器构成作为单一系统运行的服务器群集。每一服务器叫做节点；群集中的每一节点可以独立于其它节点而运行。Windows 2000 内置的群集能力是以开放规范，工业标准的硬件和易于使用的需求为基础的。

每一节点都有它自己的内存、系统磁盘、操作系统和群集资源的子集。有了叫做故障转移的进程，如果一个节点失效，其它节点就会取得失效节点资源的拥有权。群集服务器因而登记新节点资源的网络地址，从而客户的网络通信路由到现在拥有这些资源的可用系统。当失效的资源后来恢复到联机状态时，可以配置群集服务器来重新当地分配资源和客户请求。标准的 Windows 2000 群集设置如图 19.4 所示。

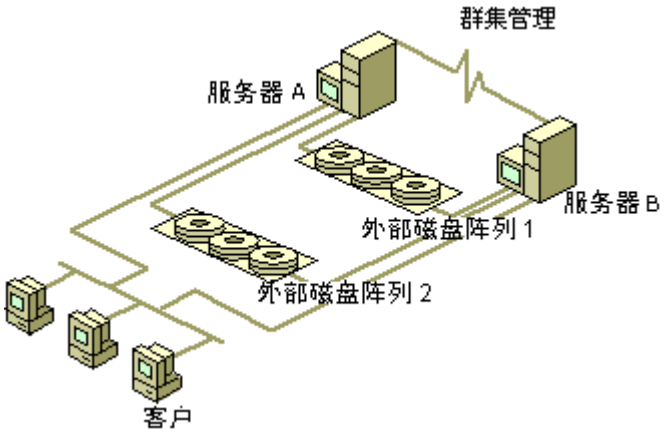


图 19.4 典型的两节点群集设置

群集服务具有下列优势：

共同管理 使用群集管理器 MMC 管理单元，作为单一系统管理群集。并且客户计算机像与单一服务器一样地与群集交互。

负载平衡 在群集内部，可以手动平衡处理负载，或者在计划的维护时卸载服务器而避免数据和应用程序脱机。

高可用性 群集能自动从许多常见的故障类型中恢复关键数据和应用程序，从而提高可用性。如果群集中的一个节点失效了，Windows 群集会检测到这一故障并恢复故障发生时正在运行的进程。群集中一个节点的故障不会影响到其它节点。

如果群集还不是您网络的一部分，或者如果您希望部署 Windows 群集，您需要在 Windows 2000 Server 部署规划阶段考虑与创建群集环境相关的几个问题。有关规划群集环境的详细信息，参见《Microsoft® Windows® 2000 Server Resource Kit Distributed System Guide》中的“Windows Clustering”，并参见 Windows 2000 Advanced Server 帮助。

备注 在实施群集方案时，请仅使用硬件兼容列表 (HCL) 中认可的配置，可以上网访问。有关这一列表的详细信息，参见 Web 资源页的 Microsoft Windows 硬件兼容列表 (HCL) 链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources。

在存储策略中使用群集的注意事项

考虑将群集环境加入到存储规划的下列优势：

- 群集提供高可用性而避免数据复制，因而在对存储需求和网络通信量影响不大的同时保证数据一致性。
- 群集具有很容易从软件故障恢复的能力。

- 服务器共享多端口磁盘阵列。硬件 RAID 控制器为外部磁盘阵列提供最好的性能。
- 群集提供高可用性的数据但是不保护数据的完整性。

文件系统改进

Windows 2000 支持 NTFS 文件系统和两种文件分配表 (FAT) 文件系统。FAT16 和 FAT32。

FAT 用于小磁盘和简单文件夹结构。FAT16 包括在 Windows 2000 中，因为它维护着与 Windows 兼容产品的早期版本的升级路径，而且它与大多数非 Microsoft 操作系统兼容。FAT32 支持大于 FAT16 处理能力的卷，并且在 Microsoft® Windows® 95 中第一次采用。Windows 2000 支持 FAT32 文件系统。

NTFS

Windows 2000 中使用的 NTFS 版本提供了 FAT 文件系统不具备的性能，可靠性和功能。NTFS 数据结构允许您使用 Windows 2000 的新功能，例如 Microsoft® Active Directory™ 服务，更改和配置管理，重解析点（目录交接点和卷的装入点），稀疏文件支持，对象 ID，扩展的性质属性，变更日志和许多新的存储增强功能。

在 Windows 2000 里，NTFS 数据结构得到更新以支持许多新的功能。对于现有的 NTFS 卷，在安装 Windows 2000 时升级到新版本 NTFS。可以在任何时间把 FAT16 和 FAT32 卷转换成这种格式。

用 NTFS 而不用 FAT 格式化 Windows NT 分区允许您使用 NTFS 特有的恢复和压缩功能。同时，用 NTFS 而不用 FAT 格式化卷还提供更快的访问速度和其它的文件和文件夹的安全功能。

重要 Windows 2000 中使用的 NTFS 版本不能被更早的版本本身识别。在 Windows NT 4.0 安装程序需要读取 Windows 2000 创建或升级的 NTFS 卷的双重引导系统中，Windows NT 4.0 安装程序需要支持（ Service Pack 4 或更高版本）。

配额管理

磁盘配额是 Windows 2000 中使用的 NTFS 版本的新功能。磁盘配额为基于网络的存储提供更精确的控制。可以按照每用户，每卷的方式使用磁盘配额监视和限制磁盘空间使用。

用户第一次试图在一个卷上存储数据的时候，他们自动输入到配额表中并分配到默认配额值。这意味着管理员不必为每个用户输入配额设置。

用户为他们拥有的文件支付费用。例如，\\Marketing\Public 上每个用户的文件夹限制为 5 兆字节 (MB) 磁盘空间。如果用户向他们的目录复制 5 MB 文件，他们就不再能在这个或 \\Marketing\Public 上的任何目录上复制或创建任何文件。但是他们可以移动和删除文件。如果用户更改别人拥有的现有文件，不向用户收取磁盘空间费用。但是记住，有些应用程序，例如 Microsoft® Office 把文件的所有者变更为最后一个编辑该文档的人。配额设置在卷之间是独立的；也就是说，C 驱动器上的配额不会影响 D 驱动器上的配额。

可以使用磁盘管理 MMC 管理单元的配额功能来：

- 在磁盘卷上启用或禁用配额。
- 防止用户在配额用完时多占磁盘空间。
- 查看卷上每个用户的配额信息。
- 设置默认配额警告阈值和分配给卷的新用户的配额限制。

- 当用户超越规定的磁盘空间限制时阻止额外磁盘分配并记录事件的发生。只要用户不试图分配更多的磁盘空间，他们可以读取，删除和编辑文件。

可以设置阈值和硬配额限制。当启用配额时，可以设置两个值：

配额限制 指定用户可以使用的最大磁盘空间。

配额警告阈值 指定当接近配额限制时且给管理员发出警告的值。这以事件提示信息的形式出现。

作为管理员，可以设定用户超越警告阈值和配额限制时自动记录事件。例如，可以将一个用户的磁盘配额设置为 50 MB，配额警告值为 45 MB。如果这个用户在卷上存储的文件高于 45 MB，配额系统记录一个系统事件。

您可选择拒绝给试图超越配额限制的用户分配磁盘空间。如果您选择这一选项，在从这一卷上删除或移走一些现存文件以前，用户不能向卷写入额外的数据。如果用户试图分配超出他们配额限制的空间，NTFS 显示“没有磁盘空间”错误提示信息。

Windows 2000 包括下列磁盘配额支持：

- 大规模远程磁盘配额管理的策略。
- 改善了的查找某特定用户拥有的所有文件的支持。

备注 Windows 2000 Server 只为格式化为 NTFS 的卷提供配额支持。

当制定存储管理策略时，考虑使用磁盘配额的下列优势：

- 每用户和每卷的磁盘空间监视方式使磁盘资源规划更好。
- 通过鼓励用户定期删除不必要的文件限制磁盘空间使得存储资源管理效率更高。
- 使用磁盘配额是减少备份媒体开销和恢复次数的有效方式。

分布式文件系统

Microsoft 分布式文件系统 (Dfs) 是能使您在企业网络上更容易地查找和管理数据的 Windows 2000 Server 软件。Dfs 为服务器、共享资源和文件的集合提供映射和通用命名规范。Dfs 增加一项功能，能把文件服务器和他们的共享资源组织成逻辑层次结构，使得管理和使用信息资源大为简化。

使用 Dfs，可以在一个组，部门或企业中创建单一目录树，将多个文件服务器和文件共享包括在其中。任何 Windows 2000 Server 都可以成为 Dfs 根目录或 Dfs 卷的宿主。Dfs 根目录是作为其它共享起始点和宿主的本地共享。网络可以包括许多有独特名称的 Dfs 卷。Dfs 拓扑是单一的域名系统 (DNS) 名称空间。可以使用单一的拓扑或多个 Dfs 拓扑来分布您所在单位的共享资源。

Dfs 的功能是和 Active Directory 集成在一起的；Dfs 拓扑发行到 Active Directory。因为对基于域的 Dfs 拓扑的更改总是自动和 Active Directory 同步，所以不管 Dfs 根目录因为何种原因脱机，总能恢复 Dfs 拓扑。基于计算机的 Dfs 在注册表中存储拓扑。

Dfs 有如下的功能：

- 提供简化的网络共享的视图，管理员可自定义。
- 允许 Microsoft® Windows® 95 和 Windows 98 客户使用服务器消息块 (SMB) 协议访问共享。

- 支持网络共享的加载复制以便平衡负载和提高数据可用性。

  Active Directory 把支持 Active Directory 的客户重定向到客户站点内的 Dfs 共享点，从而进一步优化网络使用。

- 与文件复制服务（FRS）集成来允许多个共享之间可选的读/写数据复制。

- 允许用户一次登录完成多个访问。

可以使用符合通用命名规范（UNC）的名称来访问 Dfs 卷。尽管可以使用 UNC 名称，但大多数情况下用户会发现如果他们使用一个驱动器名会简单些。例如，注意表 19.3 所示的物理位置与逻辑路径之间的对照。

表 19.3 访问 Dfs 卷

Dfs 逻辑路径	物理位置	说明	映射的驱动器路径
\\MS Server\Root	\\MS Server\Root	根目录共享	X
\\MS Server\Root\Users	\\MS Users1\Employees	employee 目录的交接点	X:\Users
\\MS Server\Root\Private\JaneD	\\Legal\Data\JaneD	JaneD 的计算机的交接点	X:\Private\JaneD
\\MS Server\Root\Private\SusanY	\\Human Res\SusanY	SusanY 的计算机的交接点	X:\Private\SusanY

因为 Dfs 把物理存储映射为逻辑表示，因而数据的物理位置对用户和应用程序都是透明的。Dfs 使用户不必了解信息存储的物理位置。因为用户不需要知道服务器或共享的名称，可以把用户信息在物理上移动到另一个服务器而不必重新告诉用户怎样寻找他们的数据，因而改善了文件的管理。

在存储策略中使用 Dfs 的注意事项

考虑把 Dfs 共享作为存储规划一部分的下列优势：

- 对于所有基于域的 Dfs 拓扑，Active Directory 把 Dfs 拓扑复制到每一个 Dfs 根服务器上。这样负载被分布到了参与的服务器上并且实现了 Dfs 根目录容错。

- 多个服务器可成为基于域的 Dfs 根目录及备用目录的宿主。如果一个根目录失效，Dfs 会检测到这个失效，另一个服务器会获得这个根目录。故障转移提高了数据可用性。

- 位于不同服务器上同一共享的多个副本可以用同一 Dfs 逻辑名加载。这为访问数据提供了备用位置，从而提供了负载平衡并提高了数据可用性。

- 共享的多个副本还允许管理员在服务器上进行预防性维护。使载有一个副本的服务器离线不会影响用户，因为 Dfs 自动把请求路由到在线的副本。

- Dfs 通过在不同站点上分布文件的副本保证用户访问最近的副本。这降低了广域网（WAN）上的负载。

- 通过允许额外的存储在子目录中发布，位置透明这一性质减轻了升级到新服务器的负担。

如果您所在单位中存在下列情况之一时考虑使用 Dfs ：

- 访问共享资源的用户分布在一个或多个站点。
- 大多数用户需要访问多个共享资源。
- 用户需要对共享资源进行不间断访问。
- 重新分布共享资源可以改善网络的负载平衡。
- 您所在单位的数据储存在多个网络共享上。

有关设计 Dfs 树的更详细信息，参见 Windows 2000 Server 帮助。

索引服务

Microsoft 索引服务使用户搜索客户机和服务器上的数据变得更简单。索引服务扫描 Windows 2000 服务器和客户机上的文件，并且建立内容和属性索引，能显著增强搜索能力和性能。这一服务运行的时候，用户可以在几秒钟内搜索数千个文件中的词汇和短语。

索引服务有如下功能：

- 内容搜索（例如，搜索所有包含“revenue projections”的文件）。
- 文档属性搜索（例如，搜索所有 AUTHOR 属性包含“Sarah”的文件）。
- 布尔操作符搜索（例如，AND，OR，NOT）。
- 使用自由文本搜索，允许输入任何词的组合而用户不必学习特殊搜索语法。
- 可以对本地计算机和网络共享卷编制索引，包括 NetWare 和 UNIX 服务器。
- 提供安全查询结果。

  只返回允许用户读取的文档。使用标准的 Windows 2000 访问控制列表 (ACL)。
- 与 NTFS 集成提供更好的性能和可靠性。
- 与 Internet 信息服务集成，为 Internet 和 Intranet Web 站点提供搜索能力。
- 可以使用 OLE-DB 或 Microsoft® ActiveX® Data Objects (ADO) 脚本创建自定义的查询表单和用户界面。
- 为许多文件格式创建索引，包括 Microsoft® Office® 97、Microsoft® Office 2000、文本文件和 HTML 页面。
- 与 Windows 2000 用户界面和 Windows 资源管理器集成。
- 使用 Microsoft 管理控制台管理单元提供简便的管理。

当索引服务在系统上运行时，它监视服务器上的文件修改。在进行文件修改时，文件打开并且内容被编制成索引。文件打开是由一个低优先级的后台进程进行的，从而对服务器的性能的影响最小。除此之外，运行 NTFS 时，索引服务使用 NFTS 的一些高级功能将总体系统开销减到最小。

备注 第一次运行该服务时，它将从头创建索引。这涉及扫描卷上的所有文件。在索引创建成功前，最初的索引构建要大量访问磁盘。在索引生成后，文件修改时只需要进行逐步更新，所以进一步的更新几乎是觉察不到的。在所有情况下，索引更新是低优先级任务，如果其它操作需要服务器资源，它就会暂停。

要搜索文档，用户只需要在 Windows 资源管理器中或从“开始”菜单选择“搜索文件或文件夹”。这将弹出搜索表单，允许用户输入要搜索的词汇。如果索引服务在文件服务器上运行，用户可以高效地搜索网络共享，因为搜索是在这一服务器上运行的，只有搜索结果通过网络返回。

与 Windows 2000 组件集成

索引服务与 Windows 2000 的其它许多组件集成以提高性能和可靠性。为保证返回搜索结果前进行快速的安全检查，此服务还使用批量 ACL 处理这样的 NTFS 功能。它还使用 NTFS 稀疏文件优化索引来避免消耗更多的磁盘空间。该服务使用 NTFS 变更日志监视卷的文件修改。这样做，该服务不会像其它许多搜索引擎那样反复地扫描整个卷。相反，当对文件进行修改时，只扫描并索引那一个特定的文件。

而且索引服务了解文件会由远程存储迁移。它不会为索引而强行地撤回这些文件。它不重新扫描被迁移到次级存储的文件。这意味着，即便文件被迁移到磁带上，用户还可以搜索它们。如果您使用远程存储为文档维护一个档案存储区，这是非常理想的。

索引服务可以被切换成只读模式。这允许管理员备份索引。在只读模式下，服务继续执行查询但是不更新索引。保证索引是一致和稳定的，从而可以创建有效的备份。备份之后，可以把服务还原为正常运行状态，备份期间对文件所做的任何修改会得到正常处理。

最后，Windows 2000 使用的全文本索引引擎和 Microsoft® SQL Server™ 7.0 的全文本索引功能兼容。在 SQL Server 中使用分布式查询处理器，可以使用结构化查询语言 (SQL) 指定查询，并且同时对文件系统和数据库同时进行操作。

在存储策略中使用索引服务的注意事项

考虑把索引作为存储规划一部分的下列优势：

- 用户可以简便而快速地从文件服务器和 Web 服务器上找到他们需要的文件。
- 尽管有供高级用户使用的强大的搜索语言，大多数用户并不需要学习搜索语法。
- 单一的文件服务器和索引可以满足对多个网络共享的查询，包括非 Windows 文件服务器上的文件查询请求。
- 因与 Windows 2000 基础结构紧密集成，性能得到改善，系统负载降低。
- 安全的搜索引擎保证用户不能找到他们无权查看或读取的文件。
- 用户界面可以使用 OLE 和 ADO 程序设计接口很容易地自定义。

如果您所在单位中存在下列情况之一时，考虑使用索引服务：

- 用户不能在服务器上找到文档或者忘记文档的位置。
- 文件服务器包含成百上千的文档，使得浏览查找某一文档很难或不可能。
- 需要为 Web 站点提供搜索功能。

加强数据保护

在企业网络中，使用一系列策略的组合来保护数据。备份和使用 Windows 2000 容错功能是加强数据保护的两种方法。

容错

容错是一个系统在部分系统失效的情况下继续运行的能力。容错处理如磁盘失效，停电或操作系统损坏这样的问题，它们会影响启动文件，操作系统自身或系统文件。Windows 2000 Server 包括容错功能。

尽管数据在容错系统中是始终可用和最新的，您仍然需要进行磁带备份来保护磁盘子系统的信息以防备用户的错误和自然灾害。磁盘容错不是带有站外存储的备份策略的替代方案。

标准的容错磁盘系统分为六个级别，称为 RAID 1 到 5 级。每个级别提供一定的性能，可靠性和开销组合。

磁盘管理

Windows 2000 磁盘管理包括 RAID 1 和 5 级。

1 级镜像卷(Windows NT 4.0 中的镜像集)

镜像卷为选定卷提供相同的副本。所有写入主卷的数据也同时写入次级卷或镜像。如果一个磁盘失效，系统使用其它磁盘的数据。因为每个文件储存在两个位置，您需要两倍于通常的空间来实现。

5 级RAID-5 卷（带有奇偶校验的带区）

RAID-5 卷在阵列的所有磁盘中共享数据。系统生成叫做奇偶校验信息的少量数据，用来在磁盘失效的情况下重建丢失的信息。RAID 5 是独特的，因为它把奇偶校验信息写入所有的磁盘。如果一个磁盘失效，通过安排数据块和阵列中的其它磁盘的奇偶校验信息实现数据冗余性。这一级别最少需要三个磁盘。随着更多的磁盘加入 RAID-5 集，开销量从最大的 50% （也就是说，需要三块磁盘储存通常两块磁盘上的数据）下降。但是，当集中有七个或更多磁盘时，在 RAID-5 集中使用多个磁盘的好处减弱。

选择 RAID 策略

RAID 策略包括硬件和软件解决方案。选择 RAID-1 还是 RAID-5 取决于计算环境。选择 RAID 策略时考虑下列因素：

- 与 RAID-5 卷相比，镜像卷的实现方式的初始成本较低，需要的系统内存少，提供的总体性能更好而且在发生故障时不会出现性能退化。但是，它的每兆字节成本比 RAID-5 卷高。
- 软件 RAID-5 卷实现读取性能更好和每兆字节成本较低，但是需要更多的系统内存而且阵列中的一个磁盘丢失时会丧失性能优势。
- 在大多数活动是读取数据的计算环境中，硬件或软件 RAID-5 卷是实现数据冗余的一个很好的方案。例如，可以在一个用于维护站点使用的全部程序副本的服务器上使用 RAID-5 卷。它保护程序以防止丢失带区卷中的一个磁盘带来的损失。而且，在组成 RAID-5 卷磁盘之间的同时读取操作使读取性能得到改善。
- 在需要对信息频繁更新的环境中，最好使用镜像卷。但是，如果您要求冗余性而且如果镜像的存储费用过于昂贵，可以使用 RAID-5 卷。

备份

备份程序帮助您防止意外的硬件或存储故障造成的数据丢失。通过备份，可以为您硬盘上的数据创建一个完全的副本，并且把数据存在硬盘或磁带这样的存储设备上。可以把数据备份到许多种类的可移动，高密度存储媒体上。而且，为便于存档，备份和远程存储集成在一起。

使用备份向导，可以：

- 为硬盘上选定的文件和文件夹创建存档的副本。
- 安排定期备份以保证存档的数据是最新的。
- 把存档的文件和文件夹还原到硬盘或其它任何您何以访问的磁盘。
- 备份 Active Directory。可以在媒体上保存一份 Active Directory 的副本以便站外存储。
- 备份脱机的远程存储数据，注册表设置和任何装入点数据。

企业网络的数据保护策略

制定数据保护策略时应考虑下列备份和容错策略：

- 备份整个卷以防备磁盘故障。一次操作恢复整个卷更有效。
- 始终备份域控制器上的目录服务数据库以防备用户帐户信息和安全信息丢失。
- 对于关键的计算机，可以实现两个独立的硬件控制的 RAID 阵列的软件镜像。使用这一配置，如果一个磁盘或者整个阵列失效，操作仍能进行。
- 为防备运行 Windows 2000 Server 的计算机发生故障，您应该准备一个安装 Windows 2000 Server 的备用计算机，以便可以把数据磁盘转移到这台计算机。

设计容错存储系统的注意事项

规划存储策略时应考虑的事项包括：

- 一般来说，只有在硬件故障或不可恢复的磁盘错误，并且主数据源因为某种原因脱机情况下，才需要容错配置以使信息随时可用。
- 如果运行 Windows 2000 Server 单一计算机上有应用程序，如果您不能容忍它们从备份中费很长时间恢复，您只需要在容错卷上运行它们便可。
- 每次您安装新的应用程序或改变应用程序的默认配置时，都要备份应用程序卷。
- 如果空间是一个考虑因素，可以使用 NTFS 文件系统格式化应用程序卷，并且在这个卷上对文件夹和文件使用 NTFS 压缩。

提高灾难恢复能力

因为即使最好的数据保护策略也无法防范计算机和站点灾难，所以应当有一个系统灾难恢复计划。灾难包括从不能启动计算机到发生自然灾害时对网络破坏等任何事件。

为了防范系统故障，您应该保存：

- 详细记录的灾难发生时恢复的计划和步骤。
- 系统活动卷或启动卷不能启动计算机时能启动计算机的软盘。
- 详细记录的计算机软件和硬件配置信息。

为减少系统恢复时间，建议执行以下任务：

- 把 Windows 2000 Server 系统和启动卷以及数据卷放在不同的驱动器上。
- 使用磁盘管理，每次改变配置时保存磁盘配置数据。
- 保存系统卷及其大小的一份书面记录。

本节的其余部分介绍 Windows 2000 的灾难保护功能，可以使用这些功能为企业防范潜在的网络灾难。

制定备份和站外存储策略

灾难恢复计划必须包括备份和恢复单个计算机和整个系统的策略和步骤。目的是为恢复数据保有一份详细的指南。

备份策略

制定备份策略时，考虑下列策略：

备份所有计算机或仅备份选定的计算机。是计划备份整个网络还是仅备份包括重要用户文件的服务器？

创建基于网络的或本地的备份。是否有通过整个网络从所有选定的服务器上读取数据的带有磁带驱动器的备份服务器，或是否所有的用户负责备份他们的数据？

使用集中的备份策略还是分布式的备份策略？是一个 IT 小组备份单位中所有服务器还是每个小组只做它们自己的备份？如果是后一种情况，您是否建立备份的时间和备份方式的指导方针？

备份计划需要包括下列活动：

- 保护存储设备和备份媒体。
- 制作所有必需设备驱动程序的副本，以保证在万一发生灾难时存储设备可以使用。恢复操作需要设备驱动程序。
- 创建和保存备份的书面副本。这些是恢复数据所必需的。
- 保存媒体的三份副本。最少在一个严格控制的站外环境中保存一份副本。
- 定期进行试验性恢复，以验证是否可以读取备份集以及包括您希望备份的所有文件。有关使用特定的备份方法和步骤的详细信息，参见《Microsoft® Windows® 2000 Server Resource Kit Server Operations Guide》中的“Backup”。

站外存储的注意事项

规划站外存储时请考虑存储下列数据和信息：

- 每周进行整个系统的完全备份。
- 所有安装过的程序和必需的驱动程序的原件。
- 保险索赔所需的文档，例如硬件和软件记录清单；以及购买定单的副本和计算机硬件和软件的收据。
- 重新安装和配置网络硬件所需信息的副本。

制定灾难恢复规划

要确定对部分或全部的数据丢失做怎样的准备，您需要确定重新创建或替代您所在单位使用的数据的总成本。考虑下列方面：

- 重建您所在单位的财务，人事和其它业务数据需要多大的开销？
- 在替代丢失数据方面的商业保险的范围是什么？
- 重建业务数据需要花费多长的时间？这折算未来业务的损失是多少？
- 服务器故障期的每小时损失是多少？

在制定全面的灾难恢复计划时有几个方面需要考虑。数据保护的计划需要回答下列问题：

- 什么数据需要备份以及每隔多久进行备份？
- 怎样保护关键计算机或在通常备份期间没有保存的其它硬件配置信息？
- 什么数据需要存储在站点内，如何进行物理存储？
- 什么数据需要在站外存储，如何进行物理存储？
- 需要什么样的培训，以使服务器操作员和管理员可以在紧急情况发生时迅速和高效地作出反应？

对恢复和还原关键数据的计划进行测试，并且在站点内和站外保存灾难恢复计划的副本。

测试系统恢复策略

测试是对灾难恢复作好准备的一个重要部分。系统管理员和操作员的技能和经验是以最少的花费和对业务最小的干扰使故障计算机和网络重新联机的一个主要的因素。需要在故障排除和执行系统恢复步骤方面对 IT 人员进行培训。

确保在引入并使用新的服务器之前测试恢复步骤。测试应该包括：

- 确保 Windows 2000 启动磁盘正常地运行。
- 测试运行 Windows 2000 Server 的计算机和集线器，路由器和其它网络组件的不间断电源供应系统。
- 测试灾难恢复计划。
- 从每日、每周和每月的备份媒体中执行完全或部分恢复。

实施恢复步骤

可以使用测试以尝试预测故障情景并执行恢复步骤。确保进行负荷测试并测试所有的功能。

您需要测试的故障包括：

- 单独的计算机组件，例如硬盘和控制器，处理器和 RAM。
- 外部组件例如路由器、网桥、交换机、电缆布线和连接器。

设置的的高负荷测试应该包括：

- 繁重的网络负荷。
- 对同一磁盘的繁重磁盘 I/O。
- 文件，打印和应用服务器的繁重使用。
- 用户的大负荷同时登录。

记录恢复步骤

需要制定在灾难后使计算机或网络重新联机的按部就班的步骤。制作操作手册，应包括下列步骤：

- 进行备份
- 执行站外存储策略
- 恢复服务器和网络

在对计算机或网络作出配置变更时应该检查该记录。在安装新版本操作系统或变更用来维护系统的实用程序或工具时，更新记录是至关重要的。

存储管理规划任务列表

表 19.4 列出了可以用来确定和满足存储需求的任务表摘要。

表 19,4 存储规划任务摘要

任务	章节中的位置
评估存储需求。	提高存储管理能力
选择数据存储系统。	提高存储管理能力
规划存储管理，包括可移动存储和远程存储。	管理磁盘资源
制定优化存储管理的策略。	优化数据管理
制定数据保护的策略。	加强数据保护
制定备份和灾难恢复策略。	提高灾难恢复能力

第 20 章 – 同步 Active Directory 与 Exchange Server 目录服务

如果您计划实施 Microsoft® Windows® 2000 Server 的 Active Directory™，而目前仍保留了 Microsoft® Exchange Server 5.5 目录服务，那么，本章对您组织中的目录服务管理人员将是很重要的规划章节。本章介绍的目录同步的概念和过程将有助您确定最划算也最有效的方式，来管理 Windows 2000 Server Active Directory 和 Exchange Server 5.5 目录服务。此外，本章的示例也将有助于您确定最适合您组织的目录同步和管理配置选项。

进入本章之前，建议您先阅读本书中“设计 Active Directory 结构”和“确定域迁移策略”两章。从中可以了解 Active Directory 的新概念和关键组件，以及域迁移的有关问题。

本章内容

目录同步概述
创建 ADC 连接协议规划
防止数据意外丢失
目录同步规划任务列表

本章目标

本章将帮助您完成以下规划文档：

Active Directory Connector （Active Directory 连接器，ADC ） 连接协议规划

资源工具包中的相关信息

- 有关 Active Directory、名称空间规划和域管理的更多信息，请参见本书的“设计 Active Directory 结构”。
- 有关迁移到 Windows 2000 的更多信息，请参见本书的“确定域迁移策略”。
- 有关 Windows 2000 Server 安全标准的更多信息，请参见本书的“规划分布式安全”。
- 有关制定测试规划的更多信息，请参见本书的“建立 Windows 2000 测试实验室”。

目录同步概述

目录同步是指保持两个独立目录服务同步的过程，比如对一个目录中的对象所做的更改将自动传播到另一目录。

Windows 2000 Server Active Directory 与 Exchange Server 5.5 目录服务间的目录同步，使您一开始就可以将 Exchange Server 5.5 的用户属性和对象迁移到一个新的 Active Directory。此外，由于 Exchange Server 5.5 支持第三方电子邮件目录服务，就可以先将第三方目录的用户属性和对象复制到 Exchange Server，然后从 Exchange Server 复制到 Active Directory。

经过了最初对 Active Directory 的迁移，这两个目录可以在生产环境中同时存在。您可以通过预先配置的自动同步操作，保持 Active Directory 与 Exchange Server 5.5 目录间的信息一致。

目录同步过程

在开始规划目录同步策略之前，不妨考虑使用图 20.1 流程图所示的规划过程。

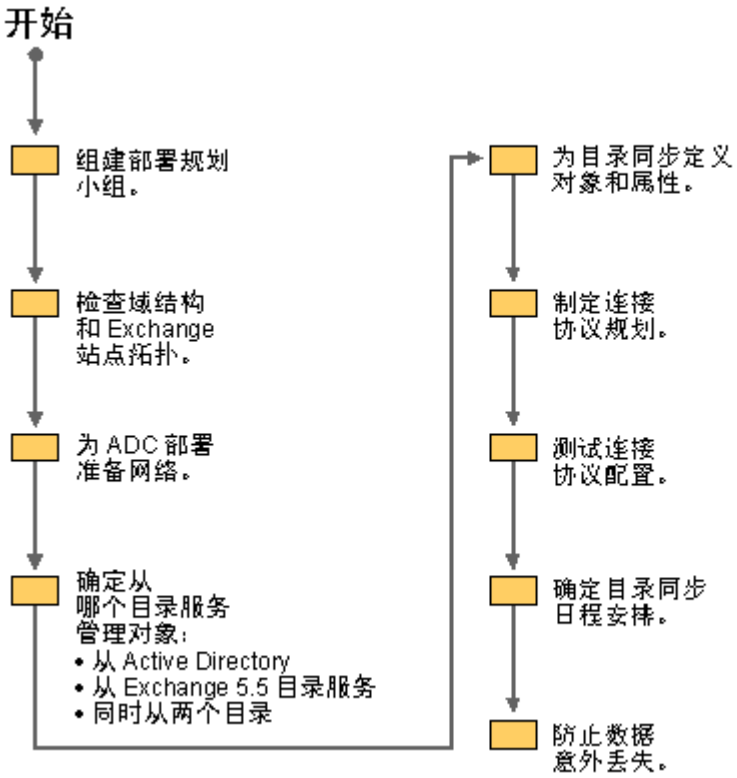


图 20.1 同步 Active Directory 与 Exchange Server 5.5 目录服务的过程

在开始目录同步规划阶段之前，重要的一点是先彻底弄清用来执行目录同步操作的关键组件。

Windows 2000 Server 软件组件

Active Directory 连接器 (ADC) 和 Microsoft 管理控制台 (MMC) 是 Windows 2000 Server 中可以用于同步和管理 Active Directory 与 Exchange Server 5.5 目录服务间通讯的软件组件。通过使用 Lightweight Directory Access Protocol （轻型目录访问协议，LDAP ），ADC 提供一种方法，可以自动保持 Active Directory 与 Exchange Server 目录服务之间信息一致。您可以使用 MMC 和 ADC 特定 MMC 管理单元及扩展工具，配置 ADC 以实现特定的功能。如果没有 ADC，您将不得不在两个目录服务中手动输入新数据和更新。

ADC 的主要特征和功能包括：

- 双向同步

  有了这一功能，最初在 Exchange Server 目录中的更改将自动传送到 Active Directory，反之亦然。这样，就可以管理源于任一目录的更改。

- 选择属性同步

  可以选择要进行同步的 Active Directory 和 Exchange Server 特定属性，而有意排除同步其它属性。

- 更改同步

  对于与 Exchange Server 的同步，Windows 2000 Server 只在对象级别更新更改。例如，如果为 100,000 个用户更改了 20 个用户对象，则系统将只更新那 20 个用户对象。这减少了复制和传输时间，也减少了网络通信量。

- 属性级更改

  在同步两个对象时，ADC 会比较其属性值以确定需要同步哪些属性。例如，如果 Exchange Server 邮箱中的电话号码被修改，ADC 会比较邮箱属性和 Active Directory 中相应的用户对象，并只同步已修改的属性。在本例中，只有电话号码被同步。

- 一致性管理工具

  通过使用 Active Directory “用户”和“计算机” MMC 管理单元，可以对用户、联系人和组进行管理。

  有关 Microsoft 管理控制台和 MMC 管理单元与扩展工具的信息，请参见“ Windows 2000 Server 帮助”。

使用 ADC 的主要优点

使用 ADC 有以下优点：

单一源的管理

一旦将 Windows NT Server 4.0 域升级到 Windows 2000 Server Active Directory，您就可以很容易并且自动地配置 ADC，将 Exchange Server 5.5 目录信息迁移到新的 Active Directory，比如对图 20.2 所示的邮箱用户属性迁移。

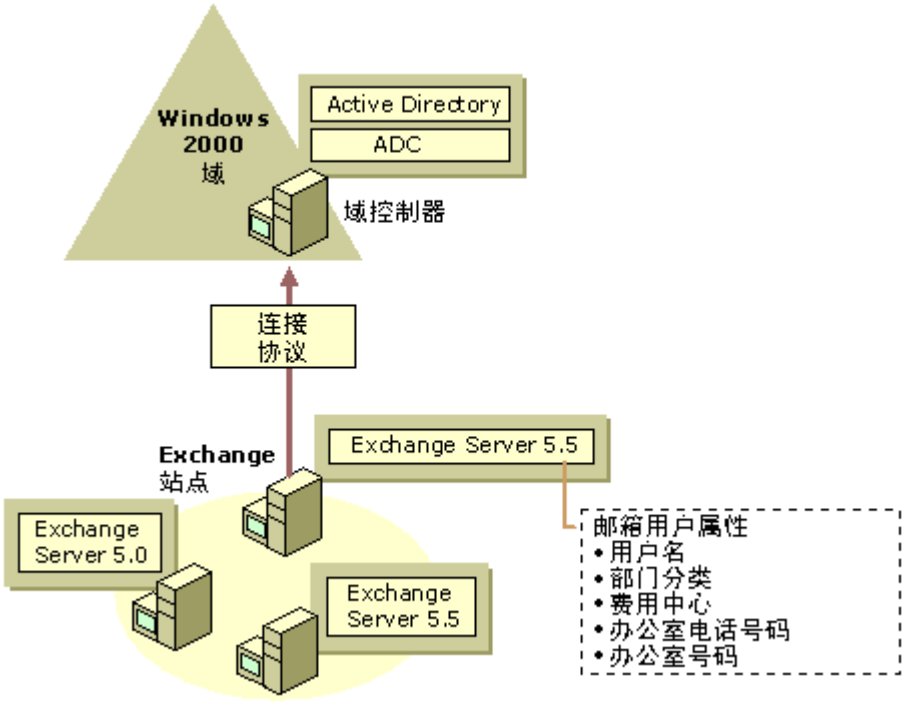


图 20.2 单一源的管理

灵便的管理和委派能力

使用 ADC，可以通过 Active Directory 来同步和管理 Exchange Server 目录，从而能够利用 Windows 2000 Server 提供的更小级别的管理委派。这意味着，有了 Windows 2000 Server，就可以在属性级别而不是在对象级别设置权限。从而允许管理员可以为不同用户委派特定属性相关的任务。

例如，用户可拥有更新所属部门费用中心、以及查看和更新部分家庭电话号码的权限。使用 Exchange Server 5.5，他们能查看属性但不能直接更新。而通过 Windows 2000 Server，目录管理员可以委派这些任务，让这些用户可以更新“费用中心”区域和家庭电话号码。您可以给授权用户委派某些任务，同时限制其访问其它数据区，如不能访问组员身份和安全权限数据区。然后可以使用 ADC 用这些授权的更改结果更新 Exchange Server 目录。

有关 Active Directory 中不同级别的管理和委派能力的更多信息，请参见本书的“设计 Active Directory 结构”。

与第三方电子邮件目录服务的协同能力

通过 Exchange Server，可以将来自第三方电子邮件目录的用户和组信息迁移到 Active Directory。Exchange Server 支持与包含目录同步代理的第三方电子邮件目录服务进行双向目录同步。图 20.3 显示了 Exchange Server 与第三方电子邮件目录服务的协同过程。

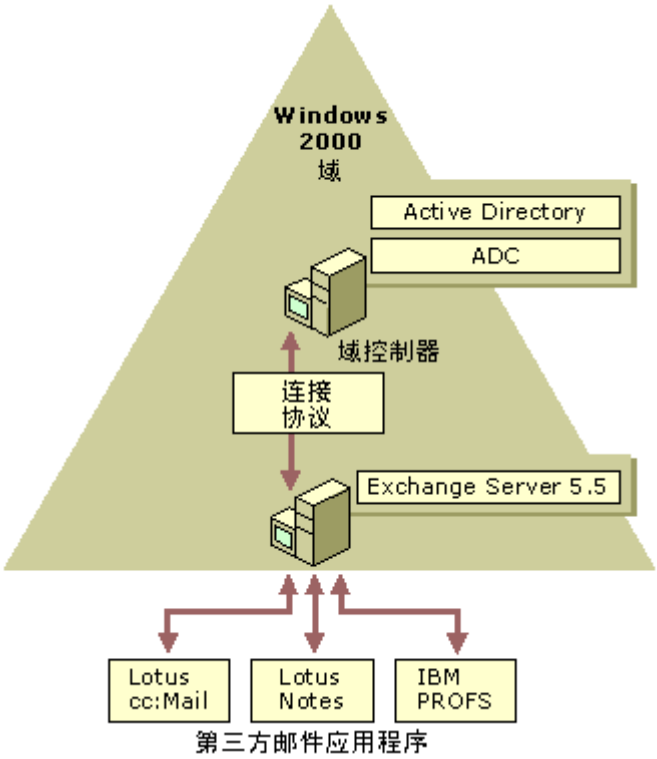


图 20.3 与第三方电子邮件目录服务的双向目录同步

网络用户的轻松定位

Windows 2000 Server 或 Windows 9x 客户只要安装了 Active Directory 客户软件，就可以使用“查找人”选项轻松找到其他用户。将 ADC 功能与 Active Directory 客户软件结合，可以将 Active Directory 快速部署为用户目录，这与使用电话目录类似。

有关 Active Directory 客户软件的更多信息，请参见本书的“为 Windows 2000 准备网络基础结构”。

使用连接协议建立关系

在服务器上安装 ADC，只是在 Windows 2000 Server 和 Active Directory 中添加了一项服务。　而要在现有 Exchange Server 站点和 Active Directory 间建立关系，必须配置一个连接协议。连接协议包含诸如以下信息：同步过程需要联系的服务器名称、要同步的对象类型、目标容器以及同步日程安排。　您可以在一个 ADC 上定义多个连接协议；每个连接协议可以从 Active Directory 到分立的 Exchange Server 站点，或者到相同的 Exchange Server 站点。

明确地说，连接协议将定义以下内容：

- 要同步的目录
- Windows 2000 Server 同步对象
- Exchange Server 5.5 同步对象
- 同步进行的方向
- 同步日程安排
- 删除对象的方式

围绕高级选项的一些细节，例如：

- 映射属性
- 创建新对象
- 验证每个目录
- 指定要同步的部门 (OU) 或容器

ADC 仅执行 Exchange Server 5.5 Service Pack 1 (SP1) 或更高版本与 Windows 2000 Server 之间的目录同步。但如果在一个 Exchange Server 5.5 站点有比 SP1 更早版本的 Exchange Server，那么该 Exchange Server 会自动与更早版本的 Exchange Server 进行同步。 这样，遍及 Exchange Server 站点和组织的所有目录信息都将是相同的。

虽然运行 Windows 2000 的一台计算机上只能有一个 ADC 服务例程处于活动状态，但还是可以建立多个连接协议。每个连接协议可以配置执行不同的同步任务。例如，一个连接协议不断更新 Windows 2000 Server Active Directory，而同时另一连接协议每天在指定时间把 Windows 2000 Server 联系人更新到 Exchange Server 目录。

制定 ADC 连接协议规划

了解了 ADC 功能和连接协议的重要性，就可以开始目录同步的规划阶段了。本节将引导您收集必要的信息，并制定自己的 ADC 连接协议规划。

组建部署规划小组

由于高度的依赖关系，协作对保证 Windows 2000 Server Active Directory 与 Exchange Server 目录服务同步平稳和有效地进行极其重要。

规划目录同步策略应该是一个合作项目，涉及关键决策人和以下各组的技术领导：

- IT 管理
- Exchange Server 管理
- Active Directory 管理
- 架构管理员组
- 网络服务

总的来说，这个小组需要充分了解 Exchange Server 站点拓扑、Active Directory 设计和网络拓扑，以避免潜在的代价昂贵的错误。

一旦组建了部署规划小组，就可以开始目录同步的规划阶段。

目录同步部署规划小组需要考虑的规划事项包括：

- 为目录同步部署小组的每位系统管理员指派明确的责任和目标。
- 确定系统管理员是否需要有关运行 ADC 和 MMC 管理单元的培训。如果需要，安排在何时进行。
- 获取安装权限

  由于对架构的写入权限只限于架构管理员组，所以必须从该组获取安装 ADC 的权限。但架构管理员只能为扩展架构目的运行 ADC 安装程序。管理 ADC 并不涉及架构，但如果需要（出于某种原因，后来的 ADC 版本涉及架构修改），将要求架构管理员组的介入和协助。有关安装 ADC 的信息，请参见本章后面的“ ADC 实现策略 ”。

  有关 Active Directory 架构的更多信息，请参见本书的“设计 Active Directory 结构 ”，并请参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide*。
- 确定何种业务流程可用这种同步操作实现进行自动化或优化。
- 获取管理层的批准以实施目录同步规划。

检查域结构和 Exchange Server 站点拓扑

开始为 ADC 连接协议规划收集信息之前，需要了解组织中的 Exchange 5.5 站点、Windows NT Server 域和 Windows 2000 Server Active Directory 结构。一旦获得了 Exchange Server 站点拓扑和域结构图，建议您考虑做以下工作：

获取 Exchange Server 站点的清单信息。需要知道有多少 Exchange Server 站点、它们是如何管理的、以及是否需要同步。对那些要同步的 Exchange Server 的站点，需要知道有关收件人容器和待同步对象的详细信息。

在 Windows 2000 Server 上安装 ADC。对每个参加目录同步的 Active Directory 域，都需要在 Windows 2000 Server 全局编录服务器上、成员服务器或域控制器上安装 ADC。

确定域中所有用户的邮箱位置。许多组织使用了多主域的域拓扑结构，用户帐户在多个域中存在。确定每个域用户邮箱的位置十分重要。最简单的情形是一个主域中的所有邮箱都放在单个 Exchange Server 站点上。

确保每个目录都有相应用于同步的对象。Exchange Server 站点邮箱可能与多个域的 Windows 2000 Server 帐户相关。您可以创建多个连接协议，连接单个 Exchange Server 站点到多个 Active Directory 域，而 ADC 会将 Exchange Server 邮箱匹配到相应的用户对象。对没有相应 Active Directory 用户对象的 Exchange Server 自定义收件人、分发列表和邮箱，ADC 会在 Active Directory 的一个域中创建新的对象。您需要决定希望 ADC 在哪个域中创建新对象。

为 ADC 部署准备网络

在运行 Windows 2000 Server 的单台计算机上只能有一个 ADC 服务例程可以活动。但 ADC 可以支持多个连接协议。要准备 ADC 部署，请考虑以下部分讲述的要求和建议。

考虑特定网络要求

为 ADC 连接协议规划收集信息时，有两个网络特定任务需要考虑。

选择作为桥头服务器的服务器。

桥头服务器负责在连接协议各个端点接收和转发电子邮件通信，类似于网关执行的任务。当选择某些服务器作为 ADC 桥头服务器时，需要它们符合以下条件：

- 有足够的资源（CPU 和内存）支持同步通信和入站 LDAP 会话的处理。
- 很好地与网络连接。例如，如果一个 Exchange Server 站点覆盖超出一个“网络集线器与辐条”网络的多个物理位置，其 Exchange Server 站点的桥头服务器必须位于网络集线器上。
- 如果 ADC 桥头服务器不是一个全局编录服务器，则必须与一个全局编录服务器同处一个局域网（LAN）段。原因在于，ADC 会试图与全局编录服务器联系以执行目标匹配搜索。当 ADC 从 Exchange Server 获取新的对象后，ADC 不会在域中随意创建一个相应的 Active Directory 对象。通过在全局编录中搜索，ADC 减少了创建重复对象的可能。
- 如果 Exchange Server 环境使用不作为邮箱主机的连接器，请考虑将这些服务器配置为 ADC 桥头服务器。

确定资源的使用情况

在目录间同步目录对象，以及在 Active Directory 和 Exchange Server 目录复制环境中的复制操作，都将消耗网络资源。

一旦 Windows NT Server 4.0 升级到 Windows 2000 Server 并与 Exchange Server 同步，Active Directory 将变为相对静态，只有一小部分数据在 Active Directory 和 Exchange Server 5.5 目录服务间传送。与同步到 Exchange Server 的 Active Directory 的更改相比，同步到 Active Directory 的 Exchange Server 5.5 目录的更改要引起稍多一些的通信量。

计算机要求

准备使用 ADC 时，请注意对计算机的技术要求：

- 必须至少有一个 Windows 2000 Server。
- 在连接协议中定义的每个 Exchage Server 上，必须安装一个 SP1 版本（至少）的 Exchange Server 5.5。

视同步日程安排的不同，ADC 服务器和其它与之相互作用的目录服务器可能会面临很大的处理负载。这些计算机的适当配置（ CPU 和内存）以及与网络的良好连接（理想情况是在同一局域网中）将十分重要。与 Exchange Server 5.x 环境中的目录复制日程安排不同，如果日程安排在用户界面上设置为“总是”，ADC 将试图在 Active Directory 与 Exchange Server 目录间同步更改。这种同步的周期是，最大连续复制时间加上 5 分钟的同步睡眠延迟。

表 20.1 显示了有 128Mb 内存并配置一个连接协议的 Pentium 系列服务器（200 MHz）的预期资源使用情况。

表 20.1 Pentium 系列服务器 CPU 的使用

CPU 的使用（大约每 5 分钟）	使用率
服务器运行 ADC	8-24%

域控制器	6-66%
连接 Exchange 5.5 桥头服务器	0-91%

要比较 CPU 类型和速度的差异，请查看表 20.2 所示的有 256Mb 内存的双 Pentium II 系列服务器 (450Mhz)的资源使用情况。

表 20.2 双 Pentium II 系列服务器 CPU 的使用

CPU 使用（大约每 5 分钟）	使用率
服务器运行 ADC	1-12%
域控制器	0-30%
连接 Exchange 5.5 桥头服务器	20-36%

对企业级 Exchange Server 5.5 和 Active Directory 的部署，需要对 ADC 及其连接协议引起的任何额外费用仔细计划。这对那些需要精确的服务器规模和网络能力的组织来说尤为重要。在 ADC 服务器、域控制器、Exchange Server 5.5 通过相对慢的链接连接时，这一点更为重要。

部署建议

为了实现成功的部署请考虑以下建议：

通过将主域控制器 (PDC) 升级到 Microsoft Windows 2000 Server 来迁移 Active Directory 用户帐户请使用 ADC 将目录数据从 Exchange Server 目录迁回到已存在的 Active Directory 帐户。这允许从 Exchange Server 同步过来的对象映射到 Active Directory 中的安全对象。

使用目录复制桥头服务器来方便 Exchange Server 站点间的 Exchange Server 目录复制。可能的话，请把它们作为连接协议的 ADC 桥头服务器。

如果可能，将托管 ADC 的服务器与 Exchange Server 目录及 Active Directory 桥头放在同一子网中。如果您在广义网 (WAN) 环境中使用 ADC，请将它放在一个战略显著位置，例如，在一个“网络集线器与条幅”拓扑的网络集线器上。

同步整个 Exchange Server 站点而不是同步单个收件人容器。可以选取整个 Exchange Server 站点作为 Exchanger Server 上的源和目标，也可以选择 Active Directory 域作为 Active Directory 一边的源和目标.这会有效将 Exchange Server 中的收件人容器层次结构与 Windows 2000 Server 的 OU 层次结构同步。以后某个时间，您可以选择更改 ADC 在 Active Directory 中创建的 OU 层次结构或单个收件人的位置。通过将收件人或 OU 移动到新的位置，下次 ADC 同步时会找到新位置并与已有收件人同步——如果 ADC 在定义的引入和引出容器搜索范围内的话。

为了获得最佳性能，将 ADC 安装在 Windows 2000 Server 域中一个成员服务器上。视同步日程安排的不同，如果将 ADC 与多个连接协议一起配置，将可能消耗很多处理时间。 如果想把 ADC 安装在域控制器或全局编录上，请确保服务器硬件能够接受附加的处理负载。

在全局编录和 Exchange Server 之间创建 ADC 连接协议，或在紧临全局编录的网络中部署 ADC.在多域环境中，即使没有连接协议用于与全局编录服务器同步，ADC 仍然依照全局编录执行搜索。在全局编录中搜索的目的在于，确保 ADC 不会在树中创建重复的对象。

ADC 实施策略

为了成功安装 ADC 并配置连接协议，您必须能够用一个带有特殊凭信的帐户登录到 Windows 2000 Server 上。 执行不同任务所需权限如下：

最初的 ADC 安装

当你最初在一个 Windows 2000 目录林中安装 ADC 时，ADC 安装程序用 Exchange 的架构扩展来扩展 Active Directory 架构。为此，运行安装所使用的帐户必须属于架构管理员组的成员，或具有扩展架构的权限。

另外，ADC 安装程序在 Active directory 配置容器中创建对象。这要求运行安装程序所使用的帐户必须属于“域管理员”组的成员，或者拥有在服务和站点容器中创建对象的权限。

最后，ADC 安装程序在本地域中创建两个安全组——一个是“ Exchange 服务”组，另一个是“ Exchange 管理员”组。这要求运行安装程序所使用的帐户必须属于“域管理员”组的成员，或者拥有在用户容器中创建对象的权限。

随后的 ADC 安装

随后在同一目录林中的 ADC 安装不需要架构管理员权限。但接下来的安装确实需要域管理员权限，或其它允许您在配置命名环境中在“站点”和“服务”容器下创建新对象的特定权限。同一域中的附加安装不要求创建 Exchange 服务或 Exchange 管理员组。但第一次将 ADC 安装到任一其它 Windows 2000 Server 域时，则需要创建这些组并需要适当的权限。

ADC 配置

您可以通过查看 ADC 管理员 MMC 管理单元中高层节点的属性页，来配置 ADC 策略。修改这种策略，就可以控制从任一目录复制来的属性组，也可以控制 ADC 用来匹配任一目录中的对象的规则组。

ADC 架构和对象映射

对两个目录间同步对象的多数属性，各连接协议都使用一个基于表格的架构地图。默认地图位于 Active Directory 中的 ADC 策略对象上。可以启用或禁用一个属性子集在任一方向的同步，但同时不能修改从 ADC 管理员 MMC 管理单元映射来的架构。

表 20.3、20.4、20.5 和 20.6 列出许多在默认架构图中定义的映射。

表 20.3 定义了 Windows 2000 和 Exchange 中所有对象的属性映射。如果需要映射的属性属性值在源目录不存在，则该映射会被忽略。

表 20.3 所有对象的属性映射

Windows 2000 属性（ LDAP 名） 所有对象类	Exchange 属性（ LDAP 名） 所有对象类
description	Admin-description
AutoReply	AutoReply
BusinessRoles	Business-Roles
Co	co
Company	company
DelivContLength	deliv-Cont-Length
department	department
displayName	cn
displayNamePrintable	name
distinguishedName	distinguishedName
dnQualifier	dnQualifier
employeeID	employeeNumber
extensionAttribute1	Extension-Attribute-1
extensionAttribute2	Extension-Attribute-2
extensionAttribute3	Extension-Attribute-3
extensionAttribute4	Extension-Attribute-4

extensionAttribute5	Extension-Attribute-5
extensionAttribute6	Extension-Attribute-6
extensionAttribute7	Extension-Attribute-7
extensionAttribute8	Extension-Attribute-8
extensionAttribute9	Extension-Attribute-9
extensionAttribute10	Extension-Attribute-10
extensionAttribute11	Extension-Attribute-11
extensionAttribute12	Extension-Attribute-12
extensionAttribute13	Extension-Attribute-13
extensionAttribute14	Extension-Attribute-14
extensionAttribute15	Extension-Attribute-15
facsimileTelephoneNumber	facsimileTelephoneNumber
generationQualifier	generationQualifier
homephone	homephone
homePostalAddress	homePostalAddress
houseIdentifier	houseIdentifier
info	info
initials	initials
l	l
Language	Language
mail	mail
mailnickname	uid
mobile	mobile
otherTelephone	Telephone-Office2
otherHomePhone	Telephone-Home2
telephoneAssistant	telephone-Assistant
pager	pager
personalPager	personalPager
personalTitle	personalTitle
physicalDeliveryOfficeName	physicalDeliveryOfficeName
postalCode	postalCode
secretary	secretary
sn	sn
st	st
street	street
streetAddress	postalAddress
telephoneNumber	telephoneNumber
telexNumber	telexNumber
teletexTerminalIdentifier	teletexTerminalIdentifier
textEncodedORAddress	textEncodedORAddress
title	title
userCertificate	userCertificate
userCert	user-Cert
userSMIMECertificate	userSMIMECertificate
url	url
x121Address	x121Address
autoReplyMessage	conferenceInformation
importedFrom	Imported-From

表 20.4 定义了 Windows 2000 和 Exchange 中所有用户对象和邮箱对象的属性映射。

表 20.4 对象类映射

Windows 2000 属性（LDAP 名） 用户对象	Exchange 属性（LDAP 名） 邮箱对象类
givenName	givenName
manager	manager
altRecipient	Alt-Recipient
publicDelegates	public-Delegates
mdbUseDefaults	mdb-use-defaults
mdbOverQuotaLimit	MDB-Over-Quota-Limit
mdbStorageQuota	MDB-Storage-Quota
submissionContLength	submission-cont-length
mDBOverHardQuotaLimit	DXA-task
protocolSettings	protocol-Settings
mapiRecipient	mapi-recipient
msExchHomeServerName	home-MDB
msExchHomeServerName	home-MTA
deliverAndRedirect	deliver-and-redirect
garbageCollPeriod	garbage-coll-period
securityProtocol	security-Protocol
deletedItemFlags	DXA-Flags
objectSID	Assoc-NT-Account
authOrig	Auth-Orig
unauthOrig	Unauth-Orig
dLMemSubmitPerms	DL-Mem-Submit-Perms
dLMemRejectPerms	DL-Mem-Reject-Perms
folderPathname	Folder-Pathname

表 20.5 定义了 Windows 2000 和 Exchange 中联系人对象和自定义对象的属性映射。

表 20.5 对象类映射

Windows 2000 属性（LDAP 名） 联系人对象	Exchange 属性（LDAP 名） 自定义对象
givenName	givenName
Manager	Manager
targetAddress	target-Address
protocolSettings	protocol-Settings
mapiRecipient	mapi-Recipient
AuthOrig	Auth-Orig
UnauthOrig	Unauth-Orig
dlMemSubmitPerms	dl-Mem-Submit-Perms
dlMemRejectPerms	dl-Mem-Reject-Perms

表 20.6 定义了 Windows 2000 和 Exchange 中组对象和分发列表对象的属性映射。

表 20.6 对象类映射

Windows 2000 属性（LDAP 名） 组对象	Exchange 属性（LDAP 名） 分发列表对象
member	member
msExchExpansionServerName	home-MTA
managedby	owner
oOFReplyToOriginator	OOF-Reply-To-Originator

reportToOriginator	Report-To-Originator
reportToOwner	Report-To-Owner
hideDLMembership	Hide-DL-Membership
authOrig	Auth-Orig
unauthOrig	Unauth-Orig
dLMemSubmitPerms	DL-Mem-Submit-Perms
dLMemRejectPerms	DL-Mem-Reject-Perms

请根据网络环境的独特性，包括部署的目标和要求以及期望的实施产出的不同，来确定组织所需的连接协议数目。您还需要熟悉那些不能同步的 Exchange Server 和 Active Directory 对象属性。表 20.7 中列出了这些属性。

表 20.7 不同步的对象属性

Windows 2000 Server Active Directory	Exchange Server 5.5 目录服务
所有帐户信息，如帐户登录、帐户密码等	高级安全设置
配置文件信息	访问控制列表 (ACL)
路由和远程访问拨号权限	主页信息存储区
访问控制列表 (ACL)	

管理对象

您需要决定从哪个目录服务来进行对象管理。如本章前面部分所述，您可以从 Active Directory、Exchanger Server 或同时从两个目录服务使用 ADC 进行对象管理。

有必要注意的是，ADC 在处理两个目录间删除对象的同步时，方式与处理其它修改对象不同。默认情况下，ADC 不会将源目录中对象的删除同步到目标目录。相反，ADC 将一个包含删除项的导入文件写到磁盘。在这个导入文件中，管理员可以看到被删除的对象，并在适当的时候，选择导入该文件，从而删除目标对象集。如果选择在两个目录间直接同步对象的删除，可以在连接协议属性页的“属性”中“删除”选项卡上选择此选项。您还可以控制 ADC 决定一个双向连接协议如何处理每个方向。

从 Active Directory 管理对象

如果决定从 Active Directory 管理对象，您需要部署每个连接协议使之可以写入 Exchange Server 目录。对于每个要从 Active Directory 进行收件人管理的 Exchange Server 站点，都必须创建从该站点到适当 Windows 2000 域的连接协议。这种管理模型可能适用的例子是，某个组织在 Active Directory 中管理雇员信息，或在其它与 Active directory 同步的目录系统中管理雇员信息。您可以使用 ADC 将雇员信息的更改更新到 Exchange Server 目录。

从 Exchange Server 5.5 目录服务管理对象

如果仍从 Exchange 管理员来管理对象，您应该将连接协议配制为“单向”，从而迁移和更新 Active Directory。可以部署只到一个 Exchange Server 站点的单个单向连接协议，并使用此连接协议将整个 Exchange Server 目录与 Active Directory 同步。这样就不需要在每个 Exchange 站点间创建和管理多个连接协议。只要连接协议配置为从 Exchange “拉”入 Active Directory，就可以选取任意 Exchange Server 站点作为源容器。

通过选取所有站点作为源容器，您可以同步 Exchange Server 目录中的整个收件人集合。这一管理模型是开始 ADC 部署的一种很好的方式。此模型将已建立的 Exchange Server 目录数据“推”入 Active Directory，而不会影响 Exchange Server 系统。一旦充分迁移了 Active Directory，并了解了 ADC 在工作环境中运行的方式，就可以将连接协议的配置修改为双向，或从 Active Directory “拉”入 Exchange。

备注 如果已经选择了多个下游 Exchange Server 站点作为单向连接协议的源，却又决定使用双向连接协议，必须从所有非本地站点中删除该连接协议的容器。为了修改任意给定 Exchange Server 站点中的对象，必须创建一个到该站点任意 Exchange Server 5.5 的独立连接协议。

从 Active Directory 和 Exchange Server 5.5 目录服务两方进行对象管理

如果从 Active Directory 和 Exchange Server 5.5 目录两方来管理对象，您必须在要同步的站点和域集之间创建双向连接协议。请务必阅读本章稍后的“设置连接协议”一节，了解有关连接协议的放置位置的信息。如果选择从两个目录管理对象，可能需要一个更加复杂的连接协议拓扑。

如果有些数据是从 Exchanger Server 管理，另一些数据从 Active Directory 管理，请使用这种管理模型。　如果同一对象在两个目录中都被修改，则会采用最新的修改。但同步这一对象可能需要两个同步周期，这要看对象是在第一个 ADC 同步周期之前还是其间被修改。

为目录同步定义对象

为 Exchange Server 5.5 目录和 Active Directory 间的目录同步定义对象的主要目标是：

- 将感兴趣的对象从一个环境提供到另一环境
- 使用户、管理员和开发人员可以方便地访问对象。

这可以通过将 Windows 2000 Server 对象（如用户、联系人和组）放入作为 Exchanger Server 镜像收件人容器的收件人容器加以实现。以下是如何做的一个示例：

在 Exchange Server 5.5 目录服务中，创建三个接收容器：

- 自定义收件人
- 邮箱
- 分发列表

在 Windows 2000 Server 上配置以下四个 OU：

- 联系人
- 用户
- 组
- 计算机

备注 由于 Exchange Server 不同步计算机，所以不需要创建对应于 Windows 2000 Server 计算机 OU 的收件人容器。

将所有公司内部用户放入“用户”容器，“自定义收件人”放入“联系人”容器中，“分发列表”放入“组”容器。最后，同步目录。

设置 Exchanger Server 容器与 Active Directory OU 间的同步有两种不同的方法。如下所述：

- 第一种方法，创建三个独立的连接协议，分别将每个 Exchange Server 容器映射到相应的 Active Directory OU。例如，Exchange Server 中的“自定义收件人”映射到

Active Directory 中的“联系人”，依次类推。图 20.4 给出了这种方法的一个示例。

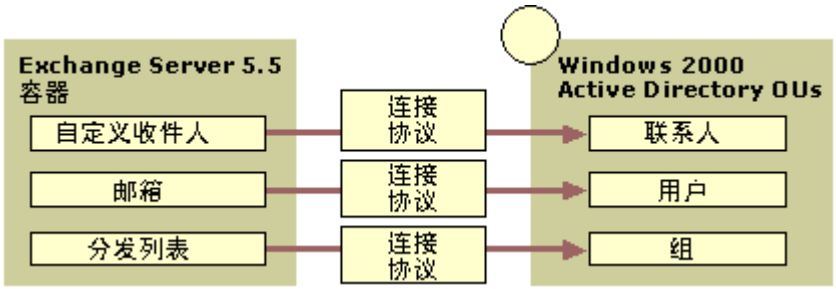


图 20.4 使用多个连接协议映射 Exchange Server 容器和 Windows 2000 Server OU

- 作为第一种方法的替换方法，您可以在 Exchange Server 全部子容器的父容器与 Active Directory 全部子容器的父容器间创建单个连接协议。在第一次同步目录时，ADC 自动在 Windows 2000 Server 的父容器下创建容器来镜像那些 Exchange Server 中容器。在这种情形下，“邮箱”、“自定义收件人”和“分发列表”会将其包含的对象复制到目录层次结构所维护的适当容器。只有包含一个或更多“邮件激活”对象的容器才被复制。

  图 20.5 示例说明了如何创建单个连接协议将数据从 Exchange Server 的指定容器映射到一个 Active Directory OU。

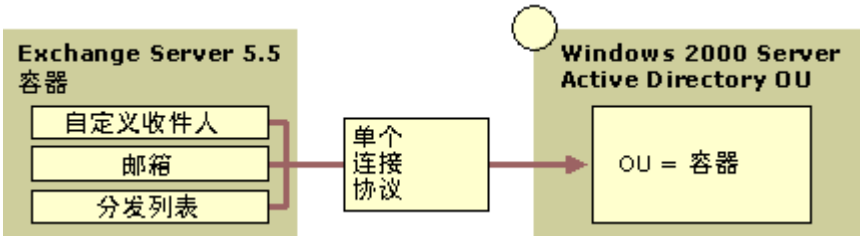


图 20.5 单个连接协议将 Exchange Server 容器映射到 Windows 2000 Server Active Directory。

建议使用第二种方式，这样可以创建较少的连接协议且系统会为你完成大部分工作。

设置连接协议

开始设置连接协议时，需要评估你的 Windows 2000 Server 域和 Exchange Server 站点，并确定理想运行状态下需要连接协议的最小数量。建议不要在企业中每个 Exchange Server 站点和 Windows 2000 Server 域之间都建立连接协议。

为了得到最佳性能，决定组织中连接协议的数量时，不妨考虑以下事项：

- 每个 Exchange server、Windows 2000 server 和 ADC server 的 CPU 速度和数量以及 RAM 的大小
- 网络带宽
- Exchange Server 邮箱和 Active Directory 用户的总数。
- Exchange Server 自定义收件人和 Active Directory 联系人的总数。
- Exchange Server 分发列表和 Active Directory 组的总数。

具体执行时，请使用 ADC 和“ Active Directory 连接器管理 ”管理单元来设置和配置连接协议。

设计连接协议

建立连接协议来同步 Exchange Server 目录服务和 Active Directory 有几种组合可以选择。要规划和创建连接协议，请用以下主要步骤：

- 确定以下描述的四种组织模型中哪种与本组织的 Windows 2000 和 Exchange Server 站点环境最匹配。
- 创建第一个连接协议设计路径来开始 ADC 连接协议规划。
- 准备好设计决定的理由，并获取管理部门开始实施的批准。

部署过程中，您将使用 ADC 和“ Active Directory 连接器 ”管理单元来创建连接协议。

备注 在以下每个 ADC 连接模型中，都假定域和 Exchange 站点处在同一个目录林中。如果域和 Exchange 站点散布在多个目录林，必须对每个目录林分别建立 ADC 拓扑。

ADC 连接模型 1：单个 Exchange Server 站点-单个 Windows 2000 Server 域

有单个 Exchange 站点的单个 Windows 2000 Server 域是 Windows 2000 Server 拓扑中最简单的域结构。一般，有单个集中的办公室且平均有 5000 个用户的较小组织可以采用这种连接模型。

图 20.6 示例说明了如何在单个 Windows 2000 Server 域与单个 Exchange Server 站点间建立一个双向连接协议。

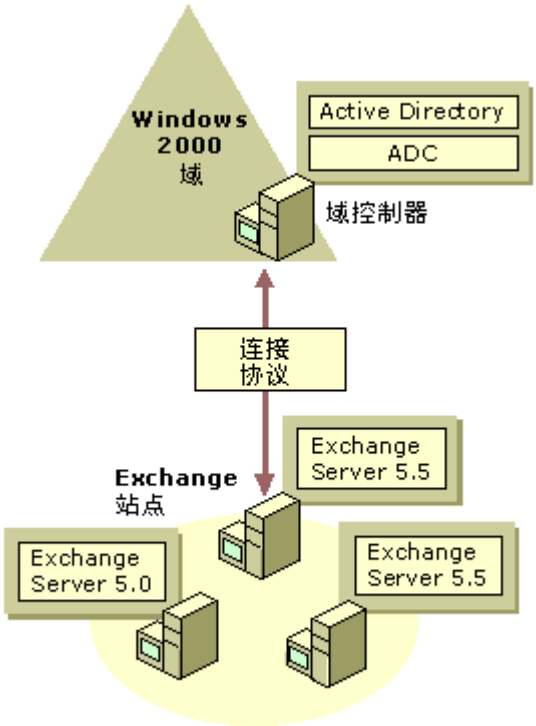


图 20.6 单个 Exchange Server 站点-单个 Windows 2000 Server 域

您可以设置连接协议以从 Windows 2000 Server Active Directory、Exchange Server 5.5、或从两方方式之一管理收件人，但不能同时以两种以上的方式管理收件人。

如果 ADC 连接模型 1 与您的组织环境最匹配，请使用图 20.7 中的流程图以帮助为组织设计 ADC 连接协议规划。

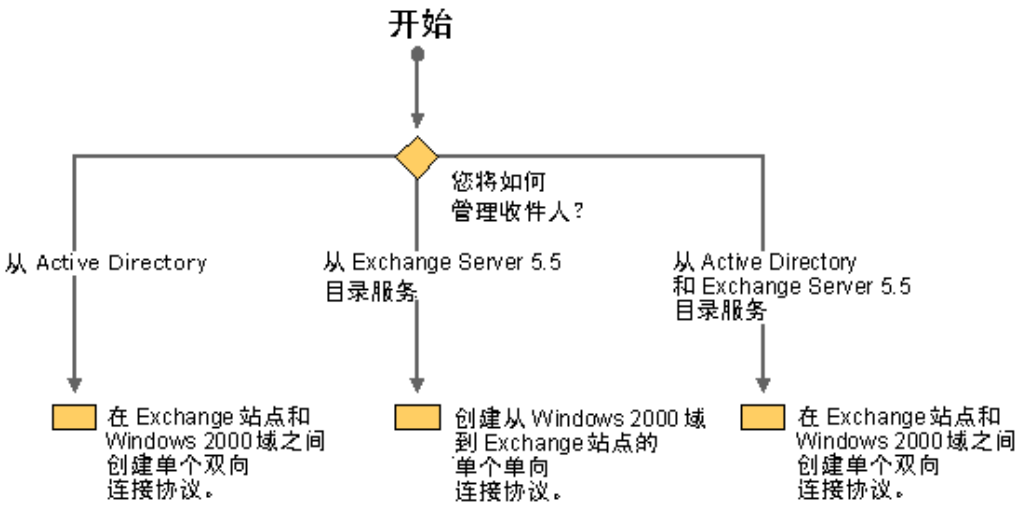


图 20.7 单个 Exchange Server 站点-单个 Windows 2000 Server 域

ADC 连接模型 2：多个 Exchange Server 站点-单个 Windows 2000 Server 域

一般的小型组织到平均有 20，000 个用户和/或多个本地和远程办公室地点的中型组织，都会发现这一连接模型将适合他们的业务需要。

图 20.8 示例说明了如何在单个 Windows 2000 Server 域和多个 Exchange Server 站点间建立双向连接协议

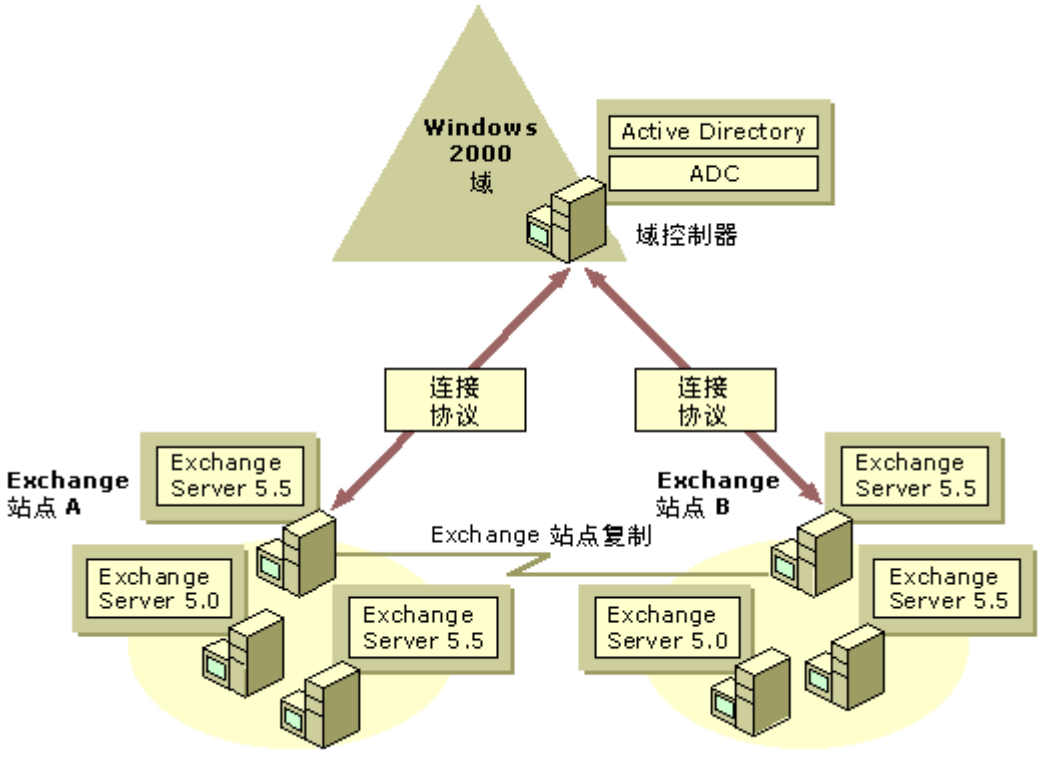


图 20.8 多个 Exchange Server 站点-单个 Windows 2000 Server 域

如果 ADC 连接模型 2 与您的组织环境最匹配，请使用图 20.9 中的流程图以帮助为组织设计 ADC 连接协议规划。

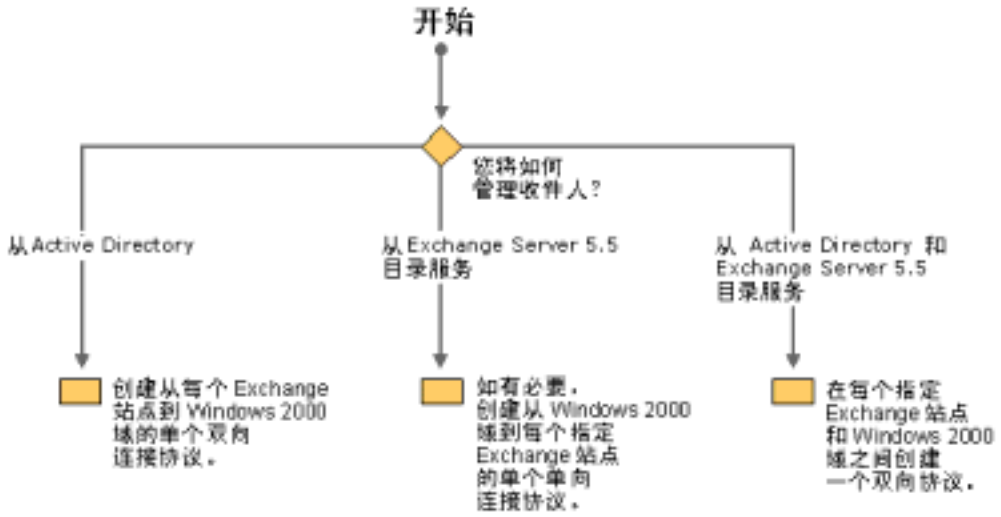


图 20.9 多个 Exchange Server 站点-单个 Windows 2000 Server 域

备注 对于有多个域和/或站点的 ADC 连接模型，需要在每个 Windows 2000 Server 域和每个 Exchange Server 站点间创建连接协议。如果在那个域中存在有主 Windows NT Server 帐户的 Exchange 邮箱，您只需要在 Exchange Server 站点和 Windows 2000 Server 域之间创建一个连接协议。

ADC 连接模型 3：单个 Exchange Server 站点-多个 Windows 2000 Server 域

对于一个中等到较大组织，或大而分散的组织的一个分部，可以为其 ADC 规划使用这种连接模型。

图 20.10 示例说明了如何在多个 Windows 2000 Server 域和单个 Exchange Server 站点间建立双向连接协议。

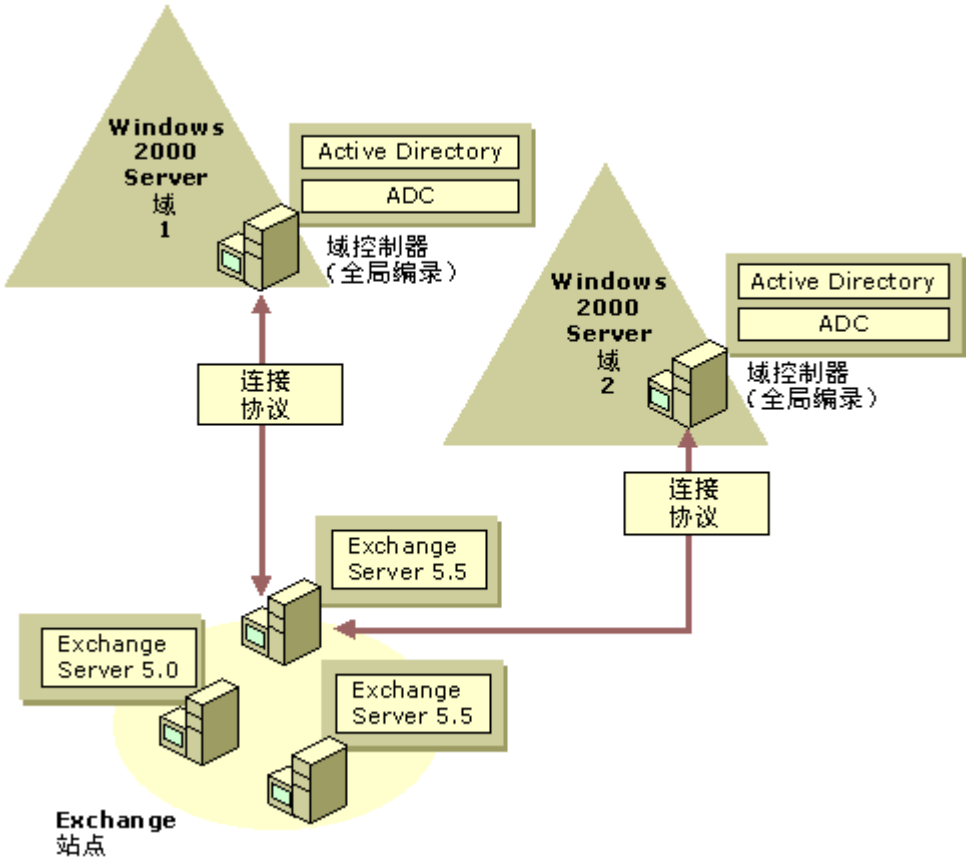


图 20.10 单个 Exchange Server 站点-多个 Windows 2000 Server 域

如果 ADC 连接模型 3 与您的组织环境最匹配，请使用图 20.11 中的流程图以帮助为组织设计 ADC 连接协议规划。 这个流程图帮助您确定如何在一个有多个 Windows 2000 Server 域和单个 Exchange Server 站点的环境中管理收件人。

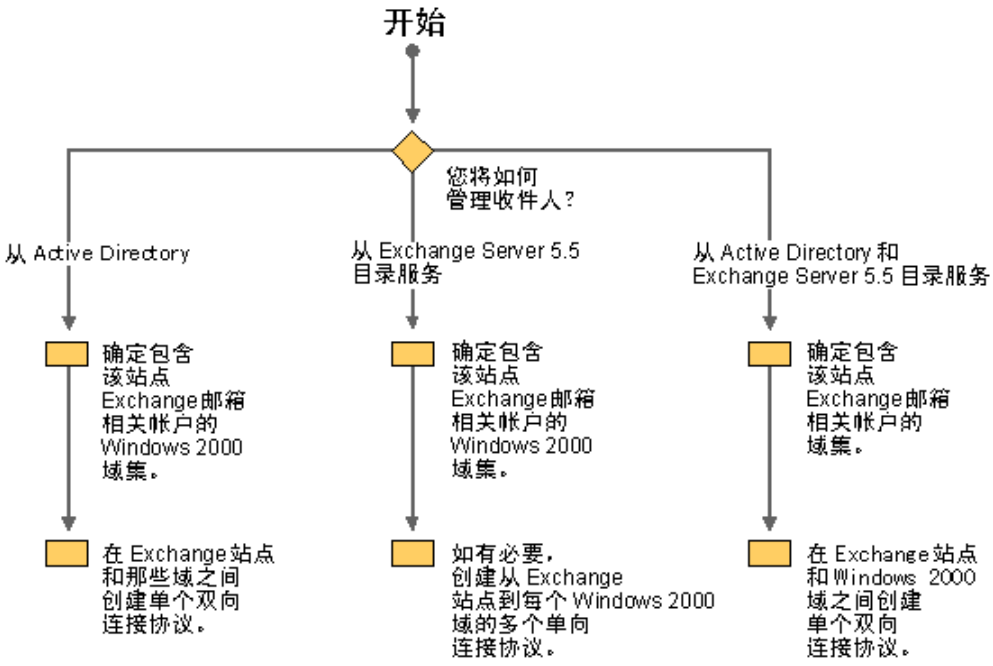


图 20.11 单个 Exchange Server 站点-多个 Windows 2000 Server 域

ADC 连接模型 4：多个 Exchange Server 站点-多个 Windows 2000 Server 域

如果您的环境有多个域和多个 Exchange Server 站点，则连接协议的设计可能会比较复杂。您需要清楚计划创建的每个连接协议的目的。

图 20.12 示例说明了如何在多个 Windows 2000 Server 域和多个 Exchange Server 站点间建立双向连接协议.

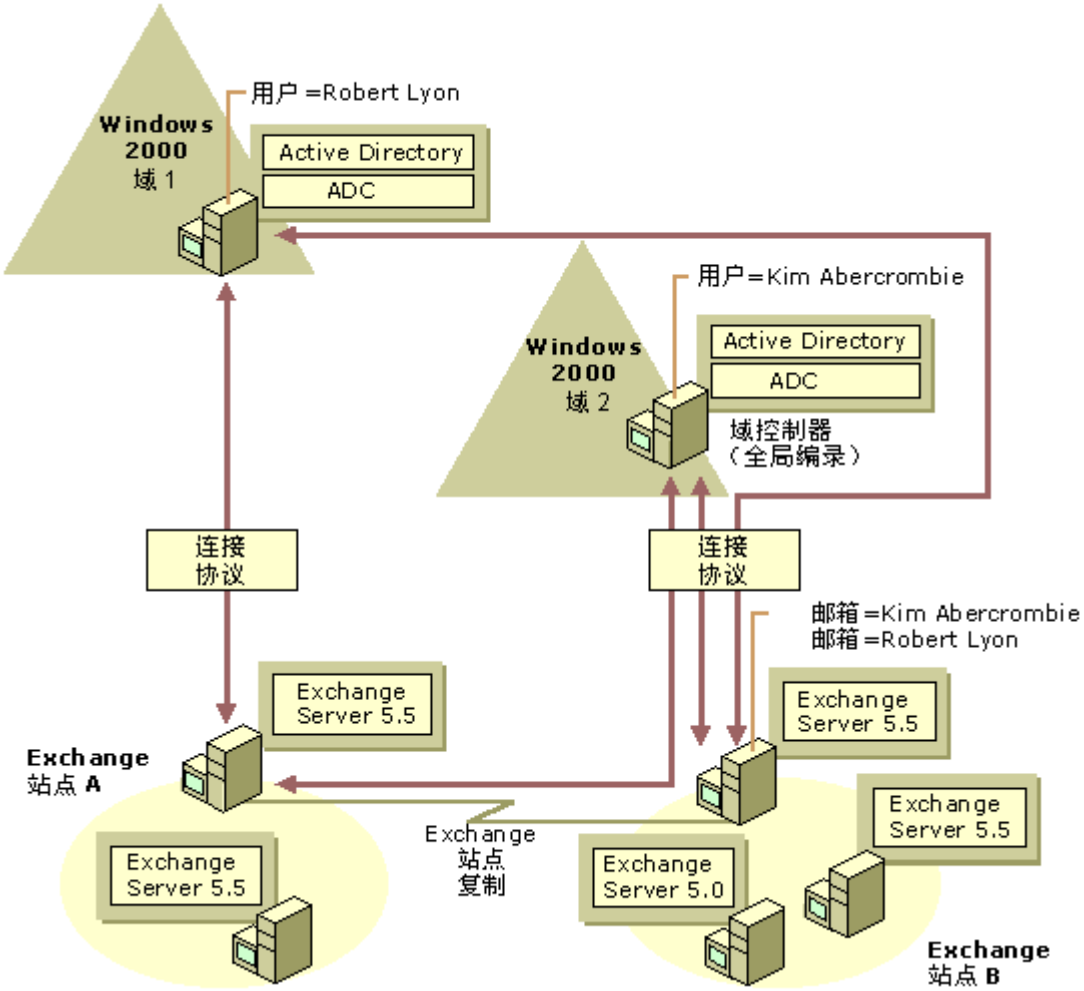


图 20.12 多个 Exchange Server 站点-多个 Windows 2000 Server 域

如果 ADC 连接了一批 Window 2000 Server 域和 Exchange Server 站点，为同步一个特定对象 ADC 可能需要多个连接协议。为了在连接协议中作出选择判断，ADC 使用一组基于邮箱在 Exchange Server 中的主 Windows NT 服务器帐户和在 Active Directory 中的相应帐户的匹配规则。如果 ADC 能将一个邮箱与其连接的任一域中的 Windows 2000 Server 帐户匹配，进而就可以同步两个对象。

例如，在图 20.12 中，Exchange Server 站点 B 上的 Robert Lyon 和 Kim Abercrombie 的邮箱与驻留在两个单独的 Windows 2000 Server 域中的用户对象进行同步。

如果 ADC 连接模型 4 与您的组织环境最匹配，请使用图 20.13 中流程图以帮助为组织设计 ADC 连接协议规划。

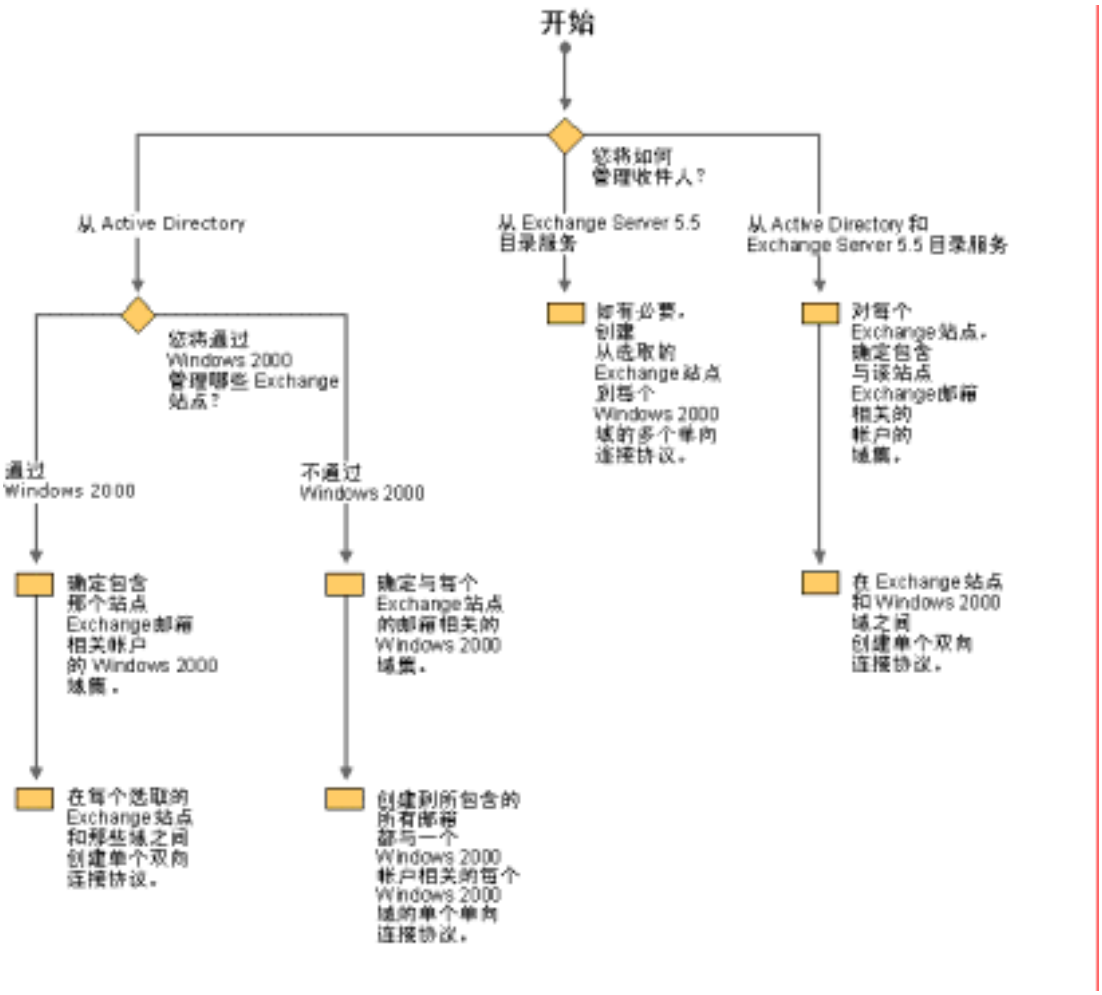


图 20.13 多个 Exchange Server 站点-多个 Windows 2000 Server 域

制定 ADC 连接协议规划文档

在这一阶段，您将与目录同步核心顾问小组和部署小组开会讨论拟订一个概要文件，包括：

- 管理员和最终用户需求
- 风险评估
- 有关 Windows NT Server 或 Windows 2000 Server 域和 Exchange Server 站点环境当前状态的报告。
- 理想 Windows 2000 Server 和 Exchange Server 站点环境的考虑事项。
- 实际 Windows 2000 Server 和 Exchange 站点环境的解决方案。

为此，请收集必要信息，创建自己的 ADC 连接协议规划。规划记录以下任务的完成情况：

- 选取前面所述的一个站点连接模型。
- 识别 ADC 网络基础结构要求并了解如何准备 ADC 实施。
- 确定用于管理对象的目录服务。
- 定义要在目录间同步的感兴趣的目标对象

请使用 Windows 2000 Server 域和 Exchange Server 站点拓扑图来创建第一个 ADC 连接协议规划路径。

测试连接协议配置

Active Directory 连接器在测试和生产环境中有截然不同的角色。请在测试环境中使用 ADC 来：

- 评估 ADC。
- 识别 ADC 的性能特征。
- 验证连接协议的布置。
- 用从生产环境 Exchange Server 目录获取的信息验证 Active Directory 的设计。

建议您创建一个测试规划。在规划测试连接协议配置时，不妨考虑以下指导方针：

- 建立一个测试实验室来镜像您的 Exchange Server 站点和 Windows NT Server 或 Windows 20000 Server 域结构。
- 如果将在原位升级 Windows NT 4.0 Server 主帐户域，请确认用以下方式在测试实验室建立 Windows 2000 Server 域控制器以便有效地测试 ADC：使生产环境 Windows NT 4.0 Server 备份域控制器 (BDC) 离线，将它们移到测试实验室，然后升级到 Windows 2000 Server 域控制器。
- 利用测试实验室环境来了解 ADC 如何将 Exchange Server 数据迁移到生产域控制器。决定这种情况下 ADC 何时将匹配已有的 Windows 2000 Server 对象，而不是创建新的 Windows 2000 Server 对象。对匹配规则做必要的调整，以确保正确迁移 Active Directory。
- 对于多域和多站点环境，测试并验证创建的 ADC 连接协议规划，并使用 ADC 桥头选项以确保正确迁移 Active Directory。
- 如要部署与 Exchange Server 一起使用的一个并行的 Windows 2000 Server 域，请测试 ADC 在为 Windows 2000 Server 规划的并行域中创建新用户的总容量。

有关制定测试规划的更多信息，请参见本书的“建立 Windows 2000 测试实验室”。

决定目录同步日程安排

您可以将单个连接协议设置成在白天或晚上的特定时间执行同步。每个连接协议有自己相应的日程安排。作为管理员，您需要为每个同步操作确定最合适的时间。一个有很多用户的网络相比一个较小的网络，可能需要更频繁的同步。同样，有些网络可能需要对特定的对象进行更频繁的同步。

以下是创建目录同步日程安排时需要考虑的一些事项：

- 决定是否将对多于 100,000 个用户或邮箱进行同步。如果是，可以通过将多个连接协议设置成在不同时间同步不同对象，以提高性能。
- 如果每天都更改一方的目录，且在第二天之前不需要这种更改反映在其它目录，应该将同步安排在夜间进行。
- 请了解 Active Directory 和 Exchange Server 目录的内部复制的日程安排。为了保证对资源有及时和有效使用，请将 ADC 同步与内部目录复制交错安排。

- 如果目录操作通常只在一周的某个或某些特定时间进行，请自定义同步过程，使其只在更改后且在更改后马上进行。

图 20.14 给出了一个生产环境和目录同步日程安排的例子。

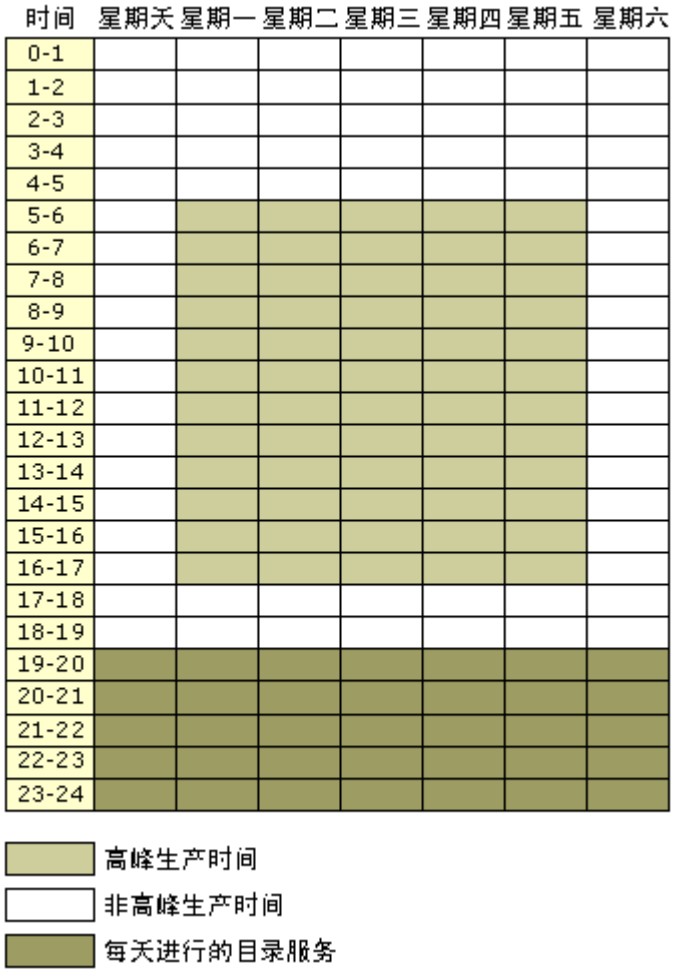


图 20.14 一个生产过程和目录同步日程安排

在创建 ADC 连接协议规划时，请创建一个类似图 20.14 的同步日程安排。附录 A 中的 ADC 连接协议规划工作表包含了一个模板，可以用来它来创建自己的同步日程安排

防止数据意外丢失

建立第一个连接协议之前，为收回目录同步操作以及备份和恢复数据制定一个规划十分重要。请与组织中的网络管理员一同制定目录同步的备份和恢复规划，这会成为主备份和恢复规划的一部分。

本节讲述了如何收回同步操作，无论数据来自 Exchange Server 5.5 目录服务还是 Active Directory。此外，您还可以找到一些有关何时备份目录的建议和帮助执行备份的工具。

有时会出现需要中途停止目录同步操作，并取消 ADC 所做的所有更改的情况。任何情况下，必须在开始故障恢复之前先删除连接协议或禁用它。将 Active Directory 恢复到原始状态的方法会因配置 ADC 连接协议同步数据的方式不同而不同。

在每种情况下，必须使用适当的 Windows 2000 Server 备份工具备份每个 ADC 连接（或正在写入）的域控制器。当然，也必须备份 Exchange Server 5.5 目录和 ADC 连接的目录。所使

用的备份工具必须支持授权还原以保证记录的恢复方式能够工作。授权还原会让一个域或容器回到备份时的状态，并覆盖备份后所做的所有更改。

有关授权还原的的更多信息，请参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide* 中的“ Active Directory 备份与还原 ”。

有两种情况可能需要收回一个正在进行的同步：

例 1：将新对象迁移到 Active Directory

连接协议被配置成将新对象（联系人和分发组）迁移到 Active Directory。在这一特殊的例子中，您将创建一个专用的 OU 只放置 ADC 创建的对象。 故障恢复的方法是删除连接协议指定的 OU。这将删除 OU 中连接协议创建的所有对象。如果任何其它 Active Directory 对象放置在该 OU（例如用户或打印机）中，OU 被删除时它们也被删除。为了防止数据丢失，删除 OU 之前必须将用户和打印机对象移走。

例 2：迁移已有对象的属性（字段）

ADC 被配置成将存储在 Exchange Server 目录中的信息迁移到已有对象的字段。可以把对象分布到域控制器的不同容器。这种情况下，取消 ADC 做的更改需要一个授权还原。这会取消 ADC 做出的更改，但可能引起数据丢失。此外，选取的域或容器中最后一次备份之后的所有其它更改也会丢失。

您可以对单个容器运行授权还原。首先您应该决定哪些容器受到影响，然后对这些容器执行授权还原。

有关灾难恢复，请参见本书的“确定 Windows 2000 存储管理策略”，或请参见 *Microsoft® Windows® 2000 Server Resource Kit Server Operations Guide* 中的“备份” 和“修复、恢复和还原”。

目录同步规划任务列表

表 20.8 中的目录同步规划表是一个章节索引表，可以帮助您找到有关创建连接协议规划的重要任务。

表 20.8 目录同步规划任务列表

任务	章节中的位置
制定 ADC 连接协议规划	制定 ADC 连接协议规划
组建规划和部署小组	制定 ADC 连接协议规划
检查域结构和 Exchange Server 站点拓扑	制定 ADC 连接协议规划
为 ADC 部署准备网络	制定 ADC 连接协议规划
考虑特定网络需求	制定 ADC 连接协议规划
确定从哪个目录服务管理对象。	制定 ADC 连接协议规划
从 Active Directory 管理对象	制定 ADC 连接协议规划
从 Exchange Server 5.5 目录服务管理对象	制定 ADC 连接协议规划
为目录同步定义对象	制定 ADC 连接协议规划
将 Exchange Server 容器与 Windows 2000 Server OU 映射	制定 ADC 连接协议规划
设置连接协议。	制定 ADC 连接协议规划
设计连接协议。	制定 ADC 连接协议规划

制定 ADC 连接协议规划文档	制定 ADC 连接协议规划
测试连接协议配置	制定 ADC 连接协议规划
确定目录同步日程安排	制定 ADC 连接协议规划
收回正在进行的同步	防止数据丢失

其它资源

- 有关 Exchange Server 5.5 的更多信息，请参见 *Microsoft® Exchange Server 5.5 Resource Guide*，它是 *Microsoft® BackOffice® Resource Kit* 第二版的一部分。
- 有关本章任何主题的更多信息，请参见 Web 资源页上的 Microsoft TechNet 链接。地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

第 21 章 - 测试应用程序与 Windows 2000 的兼容性

当准备部署新的操作系统时，由于要花的精力很大，很容易使人不能及时考虑在系统中运行的应用程序。然而，确认哪些应用程序会在部署中引发问题并在部署开始之前将问题解决是部署项目时的关键步骤。

为了保证在部署之前解决潜在的应用程序问题，应用程序测试经理应该尽早制定测试基于 Windows 的应用程序的规划。本章将指导您完成测试应用程序与 Microsoft® Windows® 2000 兼容性的过程。

本章内容

应用程序测试概述
管理应用程序测试
识别和确定业务应用程序优先级
制定应用程序测试规划
测试应用程序
跟踪测试结果
解决应用程序不兼容性问题
应用程序测试规划任务列表

本章目标

本章将帮助您完成以下规划文档：

- 业务应用程序优先次序列表
- 测试应用程序兼容性规划
- 测试跟踪和报告系统

资源工具包中的相关信息

- 有关制定测试规划的详细信息，参见本书中的“建立 Windows 2000 测试实验室”一章。
- 有关定义应用程序标准的详细信息，参见本书中的“定义客户管理与配置标准”一章。

应用程序测试概述

由于在 Windows 2000 中采用了一些基本的新技术，需要测试业务应用程序与操作系统的兼容性，这是 Windows 2000 部署项目的一部分。即使目前使用的是 Windows NT，也不能盲目地认为应用程序会在 Windows 2000 上也同样照常运行。增强功能（如改善的安全）意味着必须重新测试为旧版本的 Windows 而专门开发的应用程序。这些应用程序可能在 Windows 2000 下不能完全利用新的功能。但是，在 Windows 2000 下它们也应该像在当前操作平台上一样，需要良好运行。

业务应用程序的定义

在本章中，业务应用程序是指对经营业务有重要作用的任何应用程序。从大型业务线系统到专用工具，都属于业务应用程序。应考虑所有在客户计算机上或是在服务器上运行的应用程序，包括商业销售成品、自定义的第三方系统和内部开发的系统。

备注 虽然在本章中经常提到基于客户的应用程序，但是，这里所讲的各种方法和问题都适用于基于服务器和基于客户的应用程序两种。

如果贵单位和许多其他单位一样，那么，您可能会发现应用程序非常多，远远没有时间将所有的应用程序都测试一遍。在这种情况下，需要确定它们的优先级，然后测试对核心业务运作至关重要的应用程序。有关怎样确定应用程序优先级的详细信息，参见本章后面的“ 识别和确定业务应用程序优先级 ”。

应用程序测试过程

图 21.1 是应用程序测试过程中涉及到的步骤图解。首先，需要分出基于 Windows 的应用程序，并根据它们对业务的重要程度，确定它们的优先级。随着清查工作的展开，可以开始规划如何协调此测试。然后，随着测试的进行，需要定期向管理人员提交进展报告，并解决出现的兼容性问题。本章将详细讲述这些步骤。

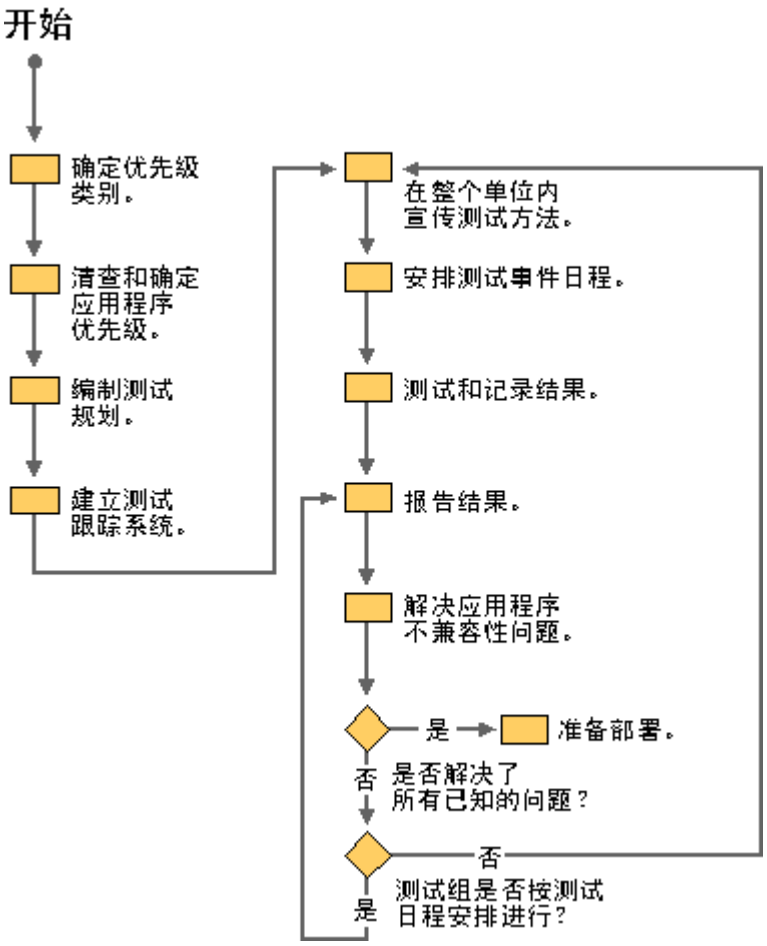


图 21.1 测试应用程序的步骤

管理应用程序测试

由于应用程序测试的工作量很大，因此，建议选择一位负责人来制定测试应用程序计划和方法，并监督测试的进度。如果贵单位是跨国企业或是位置十分分散，那么，需要在多个地方任命测试经理，尤其是当在不同地方使用不同应用程序套件时，更是如此。通过这种方法，测试经理能够有精力专心解决特定位置的需求，比如不同网络客户或性能需求。

在 Windows 2000 项目初期，应打好应用程序测试的基础，这样，可以有时间解决出现的任何问题。测试经理应协调应用程序测试项目，负责完成如下任务：

- 为确定应用程序优先级建立一个系统。
- 协调清查和确定应用程序优先级的进度。
- 制定测试方法。
- 确定测试的资源要求，包括硬件、软件和人员。
- 制定测试日程安排。
- 写出测试计划。
- 设计或购买跟踪和报告系统。
- 宣传应用程序测试的重要性和策略，与应用程序专家合作。
- 监督测试的进度，并向管理人员、内部应用程序开发组和外部供应商报告。
- 追究没有完成其测试承诺的组的责任。

识别和确定业务应用程序优先级

为测试作准备的第一个任务是收集在计算机上安装的应用程序的有关信息（包括客户和服务器）。所收集的信息（例如，此应用程序是否在使用中和有多少使用者）将帮助您确定其对业务的重要程度。

在清查应用程序时，就开始确定它们的优先级。不论有些应用程序看起来有多么不重要，都需要将每个应用程序考虑在内。任何应用程序功能不正常，都可能会对依赖它来完成工作的人们造成很大的影响。

清查应用程序

如果还没有安装在服务器和客户计算机上的应用程序清单，那么需要编制一个。别忘了将操作和管理工具包括在内，其中包括反病毒、压缩、备份和远程控制程序。

收集应用程序信息

如果贵单位很大或位置很分散，那么，编制应用程序列表是很费时间的事。如果使用 Microsoft® Systems Management Server，或是其他软件清查工具来管理网络计算机，那么可以使用软件清查进程来收集信息，然后通过运行查询进行分类并作出报告。有关使用 Systems Management Server 来编制软件清单的详细信息，参见本书中的“使用 Systems Management Server 分析网络基础结构”一章。

如果没有自动的方法弄清在计算机上安装了什么应用程序，那么需要开发一个进程来收集信息。例如，可以制作一个调查问卷或是一个基于 Web 的表单，这样，经理们就可以填写他们业务部门的软件使用的情况。如果想用人工的办法收集信息，那应得到上级管理部门的支持，来帮助您获得及时的响应。

在编制应用程序列表时，应标明哪些应用程序用于哪些业务部门。以下列表包括应该收集每个应用程序的一些信息：

- 应用程序名称和版本
- 供应商名称
- 当前状态（例如，在生产中、在开发中、或是不再使用）

- 用户数量和他们的业务部门
- 对单位的优先程度或重要性
- 应用程序运行所在的当前操作平台

  包括应用程序是基于客户机还是基于服务器的，以及哪些组件驻留在客户机和服务器中。
- Web 应用程序的 Web 站点网址（URL）
- 安装要求（例如，安全设置和安装目录）
- 开发工具或技术（如果是内部开发的）
- 联系人名称和电话号码（内部的和供应商的）

  如果同一供应商有多个联系人，那尽可能将他们合并。

在一个中心库中编制应用程序信息，这样，在收集了其他信息之后进行升级和确定应用程序优先级时，可以很容易访问和更新。当开始测试应用程序时，也可以使用这个库输入测试结果和报告状态。有关跟踪和报告测试结果的详细信息，参见本章后面的“ 跟踪测试结果 ”。

简化应用程序环境

清查过程是收集其他信息的好时机，通过这样做，可以使应用程序环境更容易管理和节省费用。将此环境越简化，就越容易测试应用程序的兼容性，迁移至 Windows 2000 就越能平稳进行，并且最终的环境就越容易管理。

本节所介绍的信息可以有助于测试，并可以降低以后的支持成本。

故障排除信息

有关应用程序的详细信息，可以帮助测试人员在测试 Windows 2000 过程中诊断问题，并可以减少帮助中心排除故障的时间。

- 安装在硬盘上的应用程序文件
- 每个文件的日期戳
- 每个文件的大小（用字节数表示）
- 文件安装位置
- 注册表设置

当在测试实验室安装应用程序时，就应考虑收集此信息，而不是在清查应用程序的时候才考虑。当在像实验室这样的可控制环境下安装应用程序时，更容易获得完全的列表，而无需在使用应用程序时慢慢积累外来的、用户特定的文件。

冗余应用程序

如果贵单位使用很多类似的应用程序，那么，清查过程是对它们进行冗余评估，和对应用最广的应用程序标准化的很好时机。例如，可能会发现，单位使用各种字处理应用程序或不同版本。对单一的应用程序和版本进行标准化可以大大简化 Windows 2000 测试及降低客户支持成本。虽然也可能有另外的小组评估和建立应

用程序标准，但测试小组应与该小组紧密合作，集中精力测试相应的应用程序。有关将客户配置标准化的详细信息，参见本书中的“ 定义客户管理与配置标准 ”一章。

未经授权的应用程序

在编制应用程序列表时，可能会发现有用户从 Internet 上下载下来的或是从家带来的未经授权的应用程序。使用清查进程来消除诸如此类的应用程序，并验证所有使用的软件是否有许可证。

站点授权的应用程序

清查过程是分出站点授权应用程序（如压缩程序和反病毒程序），并制定对其进行管理的策略的好时机。如果计划实施 IntelliMirror™，那就用它来公布这些应用程序。当用 IntelliMirror 来公布应用程序时，可以轻松地建立起冗余服务器，因此，可最大限度地提高用户对应用程序的访问效率。有关使用 IntelliMirror 进行客户支持的详细信息，参见本书中的“ 应用更改与配置管理 ”一章。

如果不准备实现 IntelliMirror，可以为站点授权的应用程序建立共享驱动器。给服务器取一个容易记住的名称，例如，\\licensed_products。

确定应用程序优先级

甚至在编制应用程序的列表之前，也可以开始设计一种分类和确定它们的优先级的方法。如果到了执行清查时，已经有了制定好的方案，那么可以在清查应用程序时对它们进行分类。您需要一个确定优先级方案，有下面两个理由：

- 在投入运行之前或许没有时间将所有应用程序都充分测试。
- 需要知道哪些应用程序是至关重要的，也就是说，对后续部署来讲，哪些应用程序是功能必须正常的。

确定优先级的最终目标是分清核心应用程序，它们必须在部署 Windows 2000 之前功能正常。当制定确定优先级的方案时，需考虑以下问题：

- 应用程序对单位的重要性
- 受影响的用户数量
- 是否有更新的版本
- 本地化需要

贵单位可能已经有了分类方案，可以使用这个分类方案或将其加以修改。例如，可能已经针对灾难恢复规划而确定了应用程序优先级。如果确定了哪些应用程序在灾难发生时必须首先联机，那么，这些应用程序在兼容性测试中具有最高优先级。

确定优先级的方案的复杂程度取决于下列因素，如有多少应用程序及它们支持的业务功能的种类。

一个大型高科技公司确定了四种优先级别。他们将优先级定义如下：

关键任务 在发生灾难之后，这些应用程序必须首先联机。需要它们来结算或履行法律义务。单位不希望这些应用程序有风险或故障风险非常小，而且故障的影响或经济损失非常高。

关键业务 在发生灾难之后，这些应用程序联机的时间顺序必须在第二位。需要它们来运行基础业务。关键业务应用程序的一个实例是人力资源应用程序。单位希望承受的故障风险很小，而且故障的影响或经济损失

适中。

要求的　要求这些应用程序运行业务，但可以脱机很长一段时间。单位希望承受适中的故障风险，而且故障的影响或经济损失较低。

其**他**　这些应用程序不属于前面的任何类别，没有它们，业务照样继续。

另一大的高科技单位只有两个类别：关键任务和非关键任务。万一没有足够的时间测试所有的应用程序，此单位想确保将所有关键任务进行完全测试，并在他们部署之前将所有问题解决。

制定应用程序测试规划

准备测试的一项主要任务是编写测试规划。在测试规划中，应指定测试的范围和目标，并阐述所要用的方法。规划中包含以下信息：

- 范围

  给其确定的测试中的优先级。

- 方法

  谁做测试及如何组织参与人员。

- 需求

  完成测试需要哪些硬件、软件、人员、培训和工具。

- 通过或不通过的标准

  决定应用程序是否通过的因素。

- 日程安排

  在预定的投入运行之前，计划如何完成测试。

根据应用程序的数量和所用的测试方法，应用程序测试可能需要本单位的各个业务部门的通力合作。早些弄清项目中应用程序测试的责任承担者，让他们审阅和同意测试规划，或是就他们的看法达成一致。

有关编写测试规划的详细信息，参见本书中的“ 建立 Windows 2000 测试实验室 ”一章。

确定测试范围

如果单位使用很多的应用程序，那么可能没有时间将它们全都尽可能彻底地测试。应当首先测试优先级最高的和最常使用或是使用最广的应用程序，但是，不要仅限于测试这些应用程序。

基于服务器和基于客户机的应用程序都要测试。由于完全是数字，所以基于客户机的应用程序通常是测试起来难度最大且最费时。

如果所使用的商业应用程序已经由外单位测试过了，但仍需要在自己的环境下进行测试。确定与基础 Windows 2000 技术兼容性的测试，未必能说明这些应用程序在您的环境下使用时运行正常。有关已在外部测试过的商业应用程序的详细信息，参见本章后面的“ 测试应用程序 ”。

定义测试方法

测试规划的一个主要部分是制定测试策略。当规划方法时，需考虑：

- 测试将在哪儿进行？
- 谁来执行测试？
- 将怎样与参与人员交流和组织他们？
- 将怎样进行测试日程安排？
- 将怎样处理应用程序问题？

应用程序测试的一个方案是外包。为了确定是否使用这个方案，应考虑如下因素：

- 有测试人员吗？
- 测试人员有适当的专业水平吗？
- 内部成本与外包成本相比，差别如何？
- 时限是多少？如果让外包来做，能否加快测试？
- 安全要求是什么？是否需要给外单位提供保密数据？

当进行内部测试时，必须选用有经验的测试人员。如果单位有一组应用程序测试人员，建议使用这些人员。如果没有这样的一个组或不能用他们，那应想办法在合理时间内利用各种资源来取得最佳效果。例如，可以让一些有经验的测试人员编写一些测试案例，这样，他们可以培训其他人来执行。另一个办法是，可以让有经验的测试人员执行测试的核心部分，然后，与业务部门协调，让他们的专家到实验室，执行他们在工作中使用的功能。

设计测试日程安排并与测试人员交流。例如，可以在 Intranet 上建立一个 Web 站点，这样，任何人都可以查看测试日期、进展报告、联系人名称和其他相关的文档。

建立一个管理测试结果的程序。明确角色和责任，应包括如下内容：

- 由谁在事件跟踪系统中输入问题报告？
- 如何确定问题的优先程度、并将它们分配下去并加以解决？
- 由谁跟踪问题解决情况和重新测试应用程序？
- 测试人员如何在测试跟踪和报告系统中输入测试结果？

案例研究 1：“ 测试节 ”

一家大型高科技单位要求其开发人员测试应用程序与 Windows 2000 的兼容性。测试经理和其他经理一起协调以让他们的小组开展合作。因为测试经理向 CIO 报告并获得对计划的全面支持，所以，对她来讲，让其他人积极参与很容易。她计划在实验室召开测试会议，并将有关会议的通知发给开发人员。实验室在建立时带有预配置计算机，可供测试人员安装应用程序。测试人员可以从 CD 或是从网络来安装他们的应用程序。为了活跃测试工作的气氛，测试经理备好了食物和饮料，因而本次会议得了个“ 测试节 ”的雅号。

案例研究 2：预览计划

一家主要的制造公司为测试 Windows 2000 Professional 制定了一项预览计划。他们使用这个计划来测试基于客户机的应用程序。此单位首先验证要在 Windows 2000 客户计算机中使用的协议堆栈与其 Windows NT 4.0 生产环境是否兼容。然后，该单位在生产网络上的不大的位置部署了 Windows 2000 Professional，用这块地方来测试应用程序。

项目组建立了一个载有关于该程序信息的 Web 站点。用户在 Web 站点上填写应用程序表单，申请加入预览计划。为了限制参与人员的数量和确保彻底测试，项目领导和人事经理审批了他们的申请。此项参与人员人数限制在 50 到 100 的计划，为应用程序测试提供了范围很广的测试人员。测试人员将问题报告张贴在 Web 站点上。

明确资源要求

在规划应用程序兼容性测试的时候，应时刻考虑到以后计算环境的状态。是否计划将一些软件或版本升级，以完全使用新的 Windows 2000 功能？是否计划实现新的标准桌面配置或是使用终端服务？像这样的问题决定所要求的资源和作为一组套件测试的应用程序。

如果计划在投入运行时用 Windows 2000 部署新的应用程序，那么，与当前的应用程序一起测试这些应用程序。

可以建立一个实验室来加快测试，这样，测试人员可以在实验室里实施测试。在这样的实验室里，应备好必须的工具和设备以供随时使用。有些单位有供测试应用程序的实验室，与 Windows 2000 实验室是分开的。如果没有建立一个单独的实验室的资金，可以与另外的项目或与培训来共用一个实验室。如果共用一个实验室，应尽量选择有大致相同的日程安排和设备需求的实验室。

在实验室里，将计算机设置为双重或三重启动，这样，测试人员可以快速进入他们需要安装和测试他们应用程序的模式。例如，如果按照本章后面“测试应用程序”中的策略建议，需要 Windows NT 4.0 和 Windows 2000 来通过升级路径测试应用程序。为了使测试人员轻松地将计算机还原到优先状态，进行驱动器磁盘映象，以带有这些基本操作系统。

考虑是否需要将实验室与企业网络连接。例如，如果开发一个基于 Web 的测试跟踪系统，那么，可能需要使用网络共享资源以便从网络或是从企业 Intranet 来安装应用程序。如果需要这样的访问，首先验证在客户计算机上使用的协议堆栈与生产网络兼容。

如果测试实验室很大，那么需要任命一名实验室经理。因为管理实验室和管理测试所要求的能力差别很大，所以，考虑选用不同的人员来担任这两种角色。实验室经理需要具有很强的技术能力，而测试经理需要具有很强的管理和沟通能力。

有关设计和管理实验室或编写测试规划的详细信息，参见本书中的“建立 Windows 2000 测试实验室”一章。

定义通过和不通过标准

当测试人员实施各种测试时，有些应用程序将会通过，而有些则会不通过。应该有一个规定好的程序，这样，参与人员可以知道他们在什么时候和什么地方记录应用程序问题和待解决的问题。

当测试人员完成对某一特定应用程序的测试后，他们需要将结果输入到测试跟踪和报告系统中去。当然，需要确定尚未解决的问题的优先级并跟踪它们，然后在问题解决之后，重新测试应用程序。但是，为了跟踪测试进度，或许想知道哪些应用程序已经准备好了，哪些还没有。如果计划按应用程序通过或不通过来跟踪进度，那么需要对使用的类别制定标准。为了制定通过和不通过的标准，需考虑如下问题：

- 问题的重要性如何？它是否影响某一关键功能或是某一非重要功能？
- 人们遇到此问题的可能性有多大？
- 有避免此问题的方法吗？

制定测试日程安排

测试日程安排取决于很多条件，包括：

- 有多少测试人员参与。
- 此项目的测试人员是专职的还是兼职的。
- 测试人员的经验。
- 应用程序的数量和复杂性。

应在日程安排中留出足够的时间，以便解决问题和对未通过测试的应用程序进行重新测试。建立主要的和临时的阶段点，这样，可以监督进度，并确认是否在按日程安排进行。

测试应用程序

Microsoft,与消费者和独立软件供应商 (ISV)一起合作，开发了 Windows 2000 应用程序规范。按此规范编制的应用程序不仅与 Windows 2000 兼容，而且它们还能利用 Windows 2000 所提供的新技术。

可以从 Microsoft Developer Network (MSDN) Web 站点下载 Windows 2000 应用程序规范，它有两个组件：一个用于桌面应用程序，另一个用于分布式应用程序。桌面应用程序规范适用于在 Windows 2000 Professional 中运行的应用程序，既可作为独立程序也可作为分布式应用程序的客户部分，分布式应用程序规范适用于在 Windows 2000 Server 中运行的应用程序。有关规范和要下载其副本的详细信息，参见 Web 资源页的“ Windows 2000 Application Specification”链接，网址是：
http://windows.microsoft.com/windows2000/reskit/webresources 。

符合 Windows 2000 应用程序规范的商业应用程序也要得到认可。经认可的应用程序通过了独立测试机构的测试，而且达到了一定的要求。例如，为获得证书，应用程序必须使用 Windows 安装服务。商业应用程序可以符合规范，但可不经认可。在这种情况下，由供应商来测试应用程序，而不是由独立的测试机构来测试。

有些单位，作为他们 Windows 2000 部署项目的一部分，在购买应用程序时，已经制定了一个遵守此规范的选择标准。如果内部开发应用程序，需考虑将规范添加到应用程序开发指导方针中去。

同时，很多商业应用程序已经经过测试，以便确定它们支持 Windows 2000 的情况。Microsoft 提供了一个 Windows 2000 应用程序的目录，在那里可以查看所使用的应用程序的状况。有关哪些基于客户或基于服务器的产品支持 Windows 2000 的详细信息，参见 Web 资源页的 “ Directory of Windows 2000 Applications ”链接，网址是： http://windows.microsoft.com/windows2000/reskit/webresources。

该目录使用如下的标志：

认可 表示应用程序由一个独立的测试机构测试，而且它能利用 Windows 2000 的新功能。

准备 表示依照供应商的说明，测试了应用程序的兼容性，而且在 Windows 2000 下受支持。应用程序不一定利用 Windows 2000 的新功能。

计划 表示应用程序计划在完全测试时符合认可标准或准备标准。

制定测试策略

应用程序测试的目标是，验证在当前操作平台中工作的所有应用程序也能在 Windows 2000 中运行。如果一个应用程序是为旧版本 Windows 编写的，那它未必能充分利用 Windows 2000 的新功能，但是，其功能在 Windows 2000 中工作情况应该和在当前操作平台中一样。

商业应用程序策略

对商业应用程序，第一步是在 Check Upgrade Only 模式中运行 Windows 2000 Professional 安装程序，以检查潜在的不兼容性。当在此模式下运行安装程序时，它将安装的软件与一组已知不兼容的应用程序列表进行对照检查，看是否存在不兼容，并将所发现的任何应用程序记录下来。Check Upgrade Only 模式的命令行语法是：

winnt32 /checkupgradeonly

虽然此工具能够警告潜在的兼容性问题，但它只针对很小一部分的应用程序，而且只针对安装在正在检查的计算机上的应用程序。即使一个应用程序不在不兼容应用程序列表中，这也并不意味着它是兼容的。有关安装程序的详细信息，参见本书中的“ 客户自动安装与升级 ”一章。

下一步是检查 Windows 2000 应用程序目录，以确定使用的应用程序是否兼容。

即使发现有些应用程序已经由其他人测试过了，也应该在环境中对它们进行测试。在这种情况下，测试要着重于单位使用此应用程序的方式。例如，测试：

- 单位使用的配置。
- 最常使用的功能。
- 一起使用的应用程序组合。

本章后面的“ 测试窍门 ”一节提供了测试应用程序功能的方法举例。如果使用的商业应用程序的兼容性未经其他机构测试过，那么，对其测试应该比测试其他应用程序更全面。

别忘了测试反病毒软件。很多这些应用程序需要升级，因为它们使用文件系统筛选器。很多 Windows NT 4.0 文件系统筛选器由于改用 NTFS 文件系统，可能不能在 Windows 2000 中运行。

自定义应用程序策略

如果使用自定义第三方产品或在内部开发应用程序，那么需要制定比已经测试过的商业应用程序更全面的测试策略。

即使测试不是您开发的应用程序，Windows 应用程序规范也可以提供测试的试金石。MSDN Web 站点中包括可下载的规范版本，以及一个详细测试规划，上面有想得到 Windows 2000 应用程序认可的所有 Microsoft 测试。此测试规划可以提供有关功能部分的思想和应该测试的方法。有关如何下载规范或测试规划的详细信息，参见 Web 资源页的“ Application Specification Download”链接，网址是：
http://windows.microsoft.com/windows2000/reskit/webresources 。

MSDN Web 站点也包括其他有关测试的重要信息，例如，有关探索性测试的白皮书和独立测试机构用来测试应用程序（这些应用程序是由供应商为获得认可而提交给测试机构的）功能的方法。

测试窍门

本节中的测试建议不很全面，而且并不是对所有的情况都适用。提供它们是为了帮助您开始考虑如何测试。

测试部署方案

应该使用在部署过程中计划使用的测试方案测试安装和运行应用程序。例如，您可能计划在没有任何东西的机器上从头安装，或是从 Windows 3.*x* 或旧版本的 Windows NT 上升级的方式来部署。如果计划升级，可以在升级的过程中将应用程序留在计算机上，或将它们卸载然后在升级之后重新安装。

考虑将应用程序为 Windows 安装服务重新打包，或保存为 .zap 文件，这样应用程序可由 IntelliMirror 软件安装程序和维护软件来管理。有关封装应用程序的详细信息，参见本书中的“ 应用更改与配置管理 ”一章。

由于 Windows 3.*x* 和 Windows 2000 之间的差异，一些应用程序的安装程序工作方式不同，这取决于使用什么操作系统来安装。例如，如果在运行 Windows 3.*x* 的计算机上安装应用程序，然后将计算机升级到 Windows 2000，那么，此应用程序运行起来可能与安装在 Windows 2000 中的不同。在这种情况下，或许需要先卸载该应用程序，然后在升级或是在获得迁移动态链接库 (DLL) 之后，重新安装。

迁移 DLL 可使原先安装在 Windows 3.*x* 上的应用程序在计算机升级到 Windows 2000 后运行正常。迁移 DLL 能够通过执行如下的操作解决应用程序问题。

- 用与 Windows 2000 兼容的文件替换或升级 Windows 3.*x* 特定的文件。
- 将应用程序和用户设置移动到 Windows 2000 中的正确位置。
- 将 Windows 3.*x* 特定的注册表项映射到 Windows 2000 中的相应位置。

对于内部开发的应用程序，或许需要创建迁移 DLL，或是从供应商处获取。通过使用关键字“ migration DLL ”在 MSDN 库中搜索，能够找到有关创建和测试迁移 DLL 的详细信息。有关 MSDN 库的详细信息，参见 Web 资源页的 MSDN 链接，网址是： http://windows.microsoft.com/windows2000/reskit/webresources。Windows 2000 中也包含有一些迁移 DLL。

因为结果在很大程度上取决于是如何升级的，所以，使用与投入运行时计划使用的过程和工具进行测试非常重要。如果在测试应用程序时过程和工具没有准备好，那么，至少要测试计划使用的方案。

升级方案

如果计划对计算机进行升级，请使用如下步骤：

- 安装 Windows 3.*x* 或 Windows NT 3.51，或更高版本。
- 安装应用程序。
- 升级到 Windows 2000。
- 测试应用程序。

如果一个 Windows 3.*x* 应用程序运行不正常，请与 ISV 联系，索取迁移 DLL。如果一个 Windows NT 应用程序运行不正常，请与 ISV 联系，索取补丁程序或是新的安装程序。

从头安装方案

如果计划在重新格式化了的计算机上安装 Windows 2000，请使用如下步骤：

- 安装 Windows 2000。
- 安装应用程序。
- 测试应用程序。

如果此应用程序运行不正常，请与 ISV 联系，索取补丁程序或是新的安装程序。

测试安装和卸载

测试应用程序的安装的方式有多种，如：

- 在安装完成之前，将其终止。
- 尝试在环境中使用的所有安装选项。
- 如果贵单位允许用户安装应用程序，那么，以管理员和 Power User 的身份测试安装，然后，测试应用程序的功能。
- 尝试卸载应用程序。
- 验证应用程序可以由管理员安装和由用户卸载。当一用户以用户身份登录时，卸载应该完成，或是不允许卸载。

测试基本应用程序功能

使用用来完成业务任务的功能、配置和应用程序套，对应用程序进行测试。例如，可以尝试如下的测试类型：

- 以用户的身份登录并测试对最终用户来说最重要的功能。测试完成业务任务所需要的特定方案。
- 以是用户组成员的几个用户的身份登录。
- 将组策略应用到系统和应用程序中。
- 测试应用程序组合，例如标准桌面配置。
- 在台式机上将几个应用程序运行几天或数星期不关机。
- 测试在 Microsoft® Office 应用程序中使用 Microsoft® Visual Basic® for Applications (VBA) 的自动执行任务。
- 测试以确定长文件名一贯得到支持。包括嵌入句点和验证前导空格是否会被去除。
- 处理大的图形文件，例如超过 1 MB 的文件。
- 在字处理文档中进行大量编辑。
- 执行快速的编辑、编译、编辑、编译开发序列。
- 测试 OLE 自定义控制 (OCX)。
- 用适用的硬件进行测试，例如，扫描仪和即插即用设备。
- 如果计划部署终端服务，那么在终端服务服务器上测试应用程序。用多个运行同样的和不同的应用程序的用户及以用户特定设置进行测试。

要下载测试计划示例，参见 Web 资源页的“ Application Specification Download”链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources 。

访问数据

尝试以各种方式访问数据，如：

- 在服务器上运行当前版本的 Windows 和在服务器上运行 Windows 2000 时访问数据。
- 测试数据库的并发使用，包括对一个记录的同时访问和升级。
- 执行复杂查询。

测试打印

用各种打印机打印各种文档，如：

- 打印带有几个源应用程序的嵌入文件的文档。
- 用长文件名打印到打印机。

使用测试工具

Windows 2000 Software Development Kit (SDK)、Driver Development Kit (DDK) 和 *Microsoft® Windows® 2000 Server Resource Kit* 中包括用来测试和调试应用程序的工具。

- *Windows 2000 Server Resource Kit* 中的 Dependency Walker，循环地扫描应用程序所要求的非独立模块。此工具检测丢失的文件、无效的文件、导入或导出的不匹配项、循环依存错误和安装在不匹配计算机上的模块。有关此工具的详细信息，参见与它在一起的帮助文件。

  Windows 2000 Server Resource Kit 中的 Apimon，监视所有应用程序编程接口 (API) 调用的运行应用程序、计数和计时。还有一种可选情况，它还能够监视页错误。Apimon 可报告如下事项：

  - 所有 API 调用的计数，以及每个调用的计时。
  - 按 API 调用发生的顺序产生的跟踪记录。

常见兼容性问题

Windows 2000 中的新技术和技巧可能会在为 Windows 的以前的版本开发的应用程序中引发错误。在 MSDN Web 站点中可以找到的 Windows 2000 Compatibility Guide 中,包括很多更改的详细描述，这些改变可能引发应用程序问题。该指南将兼容性问题分为四个方面：

- 设置和安装
- 一般性 Windows 2000 兼容性
- 应用程序稳定性
- Windows 操作平台

本小节将介绍最经常能引发应用程序问题的 Windows 2000 的修改。为旧版本 Windows 开发的应用程序可能不能充分利用新功能，例如 Active Directory 或 IntelliMirror。本小节不涉及应用程序不能使用这样的新功能时出现的问题。

可能遇到以下几个方面的问题：

系统文件保护

早期的 Windows 版本允许应用程序在安装过程中替换共享系统文件。当发生这样的改变时，用户经常遇到从程序错误到操作系统不稳定等方面的问题。

System File Protection (SFP) 是 Windows 2000 中的新功能，可防止应用程序替换系统文件。此功能验证受保护的系统文件是否为正确的 Microsoft 版本。如果文件被错误的版本替换，Windows 2000 将正确的版本还原。

可靠堆阵检查

Windows 2000 在堆阵管理器中包括几个增强功能。以前没有正确使用堆阵管理的应用程序，现在可能使它们的内存管理问题暴露。常见问题包括在内存已经释放后使用它，并误以为当将内存重新分配到一个大小较小的位置后，内存不会移动。

硬件设备列举

受支持硬件设备列表的改变，可能造成使用不再受支持的设备的应用程序出现问题。

字体列举

字体列表已经改变。因为添加了支持国际化的注册表项，有些应用程序具有多种字体显示。

注册表项改变

有些注册表项已经移动或删除。使用 Win32 应用程序编程接口 (API) 对注册表进行更改的应用程序不会有问题，但是，如果它们直接写入注册表，那么可能会有问题。

版本检查

应用程序的安装程序检查版本不正确将会有问题。应该检查应用程序所要求的最小的操作系统版本，并在那个版本上或更高的版本上安装，除非应用程序依赖特定操作系统或版本。

Windows 消息传递服务

应用程序希望由操作系统来提供的 Windows 消息传递服务 (WMS)，将会找不到这种服务。必须从 Windows Update Web 站点来获取此项服务。

文件输入/输出安全

Windows 2000 对文件输入和输出安全要求更加严格。使用文件筛选器的应用程序，例如反病毒程序，可能在 Windows 2000 中丧失重要的功能。

跟踪测试结果

虽然可能已有一个事件跟踪系统，用该系统可以在遇到应用程序不兼容时将它们输入，但仍需要一个单独的方法来跟踪应用程序测试的状态。需要能够看出诸如哪些应用程序通过、哪些应用程序未通过和哪些应用程序未测试之类的信息。

必须设计一种能容易和精确地获取测试结果的方法，这样，可以按您需要的方式制作报告。当计划方法时，请考虑如下两个问题：

- 获取数据的机制
- 要获取的数据类别

选择跟踪系统

选择获取数据的机制取决于测试规模大小、预算和可用的专业人员。可以决定购买一个测试跟踪和报告系统。很多供应商供应这方面的产品。有关出售这些产品的供应商的详细信息，参见 Web 资源页的“ Test Tracking Systems ” 链接，网址是： http://windows.microsoft.com/windows2000/reskit/webresources。另一种方法是，在 Web 上使用关键字进行搜索，例如：

- “ software testing tools ”
- “ test management tools ”
- “ automated testing tools ”
- “ testing tools ”

在作出决定之前，要研究各种方案，并将现成的方案成本与自己开发的进行比较。

如果决定开发自己的系统，建议在数据库中获取数据，而不要在电子表格或字处理文档中获取。数据库在报告方面灵活性最大，而且随着数据量的增长，管理起来最容易。一个 Web 前端，不论是输入数据还是查看状态，都使用起来最方便。

自动的、联机方案的优点是可以很容易记录结果和创建报告。缺点是它需要时间开发和专业人员。因为基于纸张的系统有一些主要缺点，所以不建议使用这种方法，如使用起来不方便和制作及时的、精确的报告很困难。

不论是开发还是购买此系统，决定使用的机制应满足下面这些标准：

- 容易准确地输入数据。
- 对所有需要输入或浏览数据的人员容易使用。
- 容易备份或复制以便安全保管。
- 容易选择和将数据排序以便制作各种报告。
- 能够处理大量的数据。
- 能够同时处理多个用户。
- 保护发生改变的现有的项目。

测试人员需要一个简单的、容易记住的步骤以在完成他们的测试时来记录数据。可以链接到测试计算机上的应用程序或 Web 站点。

如果在 Intranet 上建立一个 Web 站点来收集数据，那么可以用此站点作为测试交流中心。包括进展报告、联系人名称、测试日程、到相关的信息和其他相关文档的链接。

为了建立数据收集机制，需要资源来建立如下的东西：

- 数据输入应用程序的 Web 或一些其他应用程序代码。

- 数据库和架构
- 报告和查询
- 安全，（如果需要的话）

获取数据

一旦决定如何收集数据，那么需要决定收集什么样的数据。您会发现花点时间预先确定需要什么样的数据是很值得的。如果从一开始就收集数据，那么可按您需要的方式设计新的报告。

当清查完应用程序后，您会收集到很多需要的信息。此外，可能需要每个应用程序的如下信息：

- 测试人员的姓名和业务部门
- 开发人员的姓名和业务部门（如果是内部开发）
- Windows 2000 产品名称（Server 或 Professional）

  测试结果，例如：

  - 通过
  - 不通过
  - 正在进行
  - 未知
- 输入到事件跟踪系统中的每个问题的编号
- 备注
- 每个记录的日期和时间戳

  日期/时间戳为制作某一特定时间范围内的报告提供有用的筛选。

报告结果

对所收集的数据分析得越仔细，那准备报告时就越灵活。下面的建议是一个报告的样本，可能对您有用：

- 兼容性测试不通过的应用程序列表。

  此报告要求解决问题和重新测试应用程序的后续措施。
- 按每个业务部门分，每个优先级的应用程序的总数。
- 按每个业务部门分，未经测试的应用程序总数。

  包括未测试应用程序的百分比。可以用此报告来跟踪谁在继续和谁没有继续。不要忽略用此报告作为激励那些在测试中落后的组加油的手段。

如果您按应用程序通过或不通过来报告进度，应考虑是否需要显示相对进度或实际数量。可以用诸如颜色或图形来强调显示进度。这可以使看的人看起进度来一目了然，而用数字表示可能使人容易误解。如果需要用

实际的数字来表示进度，那么或许应想出一种方法，根据应用程序的优先级，来计算或报告数字。例如，如果一个报告中只有 10 个应用程序通过和一个不通过，那么可能反映的情况不够准确。如果 10 个应用程序是由一些用户不经常使用的特殊工具，而且未通过的那个是一个对日常业务至关重要的应用程序，那么，说明此报告没有反映真实情况。

如果测试人员将问题张贴在特定的地方，如在 Web 站点上，那么必须提供一个已解决的和尚待解决的问题的报告。

在每次测试之后编写报告并将报告分发到管理部门和测试参加人员，并根据需要定期进行。如果测试项目设有 Web 站点，那么上面应能够运行联机报告。

解决应用程序不兼容性问题

当遇到应用程序不兼容性问题时，需要确定它们的优先级，然后安排人员将它们解决。应有一个如何分配问题的计划。例如，商业应用程序和内部开发的应用程序处理方式不同。安排合适的人员来研究和解决问题对应用程序测试是否成功至关重要。问题解决包括的活动范围很广，如：

- 已知问题和解决方案的研究 Web 站点。
- 和供应商联系，索取补丁程序、安装程序或迁移 DLL。
- 和 Microsoft 产品支持服务部门联系。
- 调试内部开发的应用程序。

在调查引起问题的原因时，应考虑各种方法来制定出最有效的解决办法。例如，可以选择：

- 如果是内部开发的应用程序，将问题解决。
- 如果此应用程序是购买的，那就要求供应商来解决问题。
- 用新版本或新的应用程序来替换此应用程序。
- 如果有饶过此问题的方法，那就将故障忽略。

一定要确保在将问题作为 Windows 2000 兼容性问题研究之前，它不会在当前的操作平台中发生。研究 Windows 2000 兼容性问题的一些资源是：

- Windows 2000 应用程序规范

  有关如何下载该规范的详细信息，参见 Web 资源页的“ Application Specification Download”链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources 。

- Windows 2000 Compatibility Guide

  可在 MSDN 和 Technet 中获得的此指南，包括有关诊断兼容性问题的有价值的信息。

- Microsoft Technet

  此资源含有产品更新、白皮书和其他技术信息的内容。有关 Technet 的详细信息，参见 Web 资源页中“ Technet ”链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources .

- Windows 2000 应用程序目录

这里包括支持信息和链接到供应商的 Web 站点。有关此目录的详细信息，参见 Web 资源页“ Directory of Windows 2000 Applications ”链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources。

应用程序测试规划任务列表

表 21.1 总结了在计划和测试应用程序与 Windows 的兼容性时需要执行的任务。

表 21.1 应用程序测试规划任务列表

任务	在本章中的位置
清查业务任务所用的应用程序。	识别和确定业务应用程序优先级
考虑减少使用应用程序的数量和考虑开发桌面标准。	识别和确定业务应用程序优先级
开发一个用来确定应用程序优先级的系统。	识别和确定业务应用程序优先级
根据对经营业务的重要程度来确定应用程序优先级。	识别和确定业务应用程序优先级
编制一个测试规划，包括测试方法、实验室和测试资源要求和日程安排。	制定应用程序测试规划
为获取和报告结果，开发一个测试跟踪系统。	跟踪测试结果
宣传测试方法。	制定应用程序测试规划
安排测试事件。	制定应用程序测试规划
测试应用程序和记录结果。	测试应用程序
报告测试进度。	跟踪测试结果
解决应用程序不兼容性问题。	解决应用程序不兼容性问题

其它资源

- 有关测试和诊断应用程序不兼容性问题的详细信息，参见 Web 资源页的“ Microsoft Knowledge Base”链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources 。

  有关测试应用程序的详细信息，参见：

  - *Testing Computer Software* by Cem Kaner, Jack Falk and Hung Quoc Nguyen, 1993, New York, NY:Van Nostrand Reinhold
  - *Black-Box Testing:Techniques for Functional Testing of Software and Systems* by Boris

Bizer, 1995, New York, NY:John Wiley & Sons

- *Software Testing:A Craftsman's Approach* by Paul Jorgensen, 1995, Boca Raton, FL:CRC Press
- *The Craft of Software Testing:Subsystem Testing Including Object -Based and Object-Oriented Testing* by Brian Marick, 1995, Englewood Cliffs, NJ:Prentice Hall

第 22 章 - 定义客户连接策略

本章的目的是帮助您确定企业环境中的客户计算机配置与 Microsoft® Windows® 2000 Server 网络的连接策略。参与企业网络逻辑设计的人员需要熟悉本章中所列举的建议。这些建议对大、小公司都适用。

为充分理解本章的内容，您应对基于Windows 的客户及网络有一个基本的了解。同时还应该熟悉 TCP/IP 寻址方法、远程联系方法、路由和远程访问服务。对 NetWare 网络及其协议有所了解也将是有益的。

本章内容

客户连接概述
基本客户连接
高级客户连接
远程网络连接方法
计划客户连接任务列表

本章目标

本章将帮助您完成以下规划文档：

- 客户计算机配置的连接策略。

资源工具包中的相关信息

- 有关 Windows 2000 TCP/IP 的详细信息，请参见 《Microsoft® Windows® 2000 Server Resource Kit TCP/IP Core Networking Guide》。
- 有关 Windows 2000 路由和远程访问的详细信息，请参见 《Microsoft® Windows® 2000 Server Resource Kit Internetworking Guide》。

客户连接概述

网络的规模及类型，根据它们的功能而有所不同。客户与网络的连接方法取决于他们所在的位置。举例如下：

- 内部的客户物理上都处于企业基础结构内部。内部的客户可利用多种多样的网络媒体，如异步传输模式 (ATM)、以太网和令牌环。
- 外部的客户远离公司网络设施，因此需要路由和远程访问或虚拟专用网络。

客户应能连接多种多样的资源。这些资源包括：文件和打印服务器、数据库服务器，比如 Microsoft® SQL Server™、Microsoft® Exchange Server，以及内部 Web 服务器。

为保证客户的连接高效、可靠，必须先确定 Windows 2000 客户连接策略，然后您才能实施连接计划。图 22.1 概括地说明了确定客户连接策略的基本过程。您不必依照图上所列举的顺序来执行这些任务。这个流程图提供需要执行的任务清单，同时给出一个可以完成这些任务的顺序的建议。

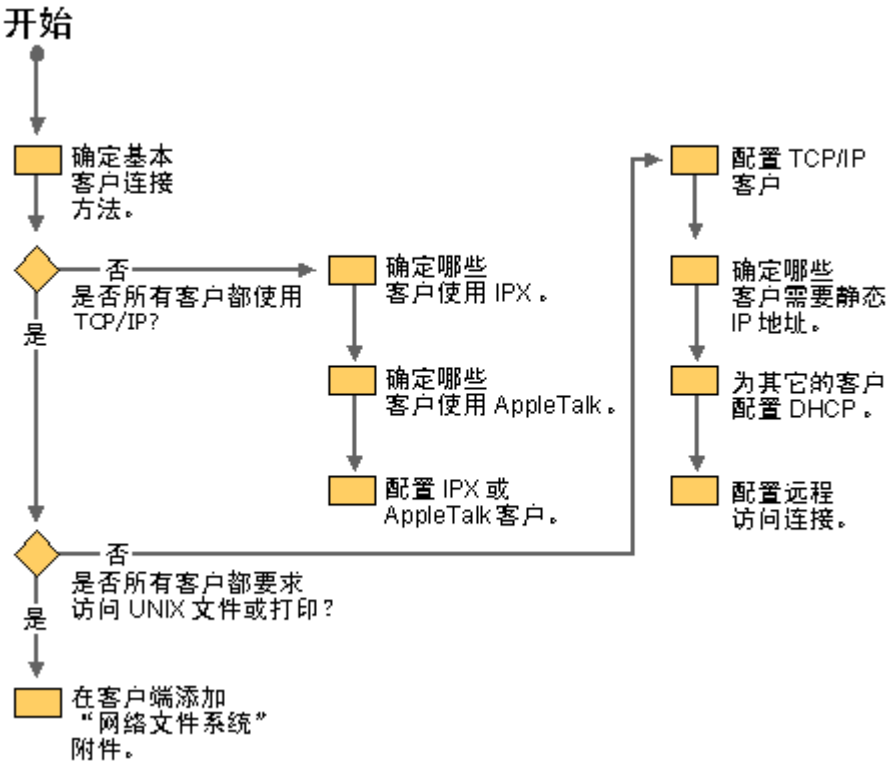


图 22.1 确定客户连接策略的过程

基本客户连接

当您将运行 Microsoft® Windows® 2000 Professional 的计算机连接到一个局域网 (LAN)，Microsoft Windows 2000 操作系统将检测出您的网络适配器，并建立一个局域网络连接。如同其它连接类型，它将出现在“网络和拨号网络连接”文件夹，可从“控制面板”进入该文件夹。默认情况下，局域网连接是唯一自动激活的连接。拨号连接将不会被系统激活。需要通过“控制面板”中“网络和拨号网络连接”文件夹中的“网络连接向导”对它们进行手动配置。

局域网络连接包括：以太网、令牌环、电缆调制解调器、数字用户线路 (DSL)、光纤分布式数据界面 (FDDI)、ATM IP、红外数据协会、无线及 ATM 仿真 LAN。仿真 LAN 基于虚拟的适配器驱动程序，如 LAN 仿真协议。

如果您更改网络，可通过修改现有的局域网络连接设置，来体现出这些变化。这些更改可以用以下形式：

- 协议，如静态 IP 地址的更改。
- DNS 或 WINS 配置。
- 服务。

通过“状态”对话框，您可以浏览局域网络的连接信息，如连接持续时间、连接速度、发送和接受的数据量，以及某一特定连接可使用的诊断工具。可以把局域网络的状态图标加到 Windows 任务栏。

如果在客户上安装了新的 LAN 设备，当您再次启动 Windows 2000 时，在“网络和拨号网络连接”文件夹中将出现一个新的局域网络连接图标。对膝上型电脑，可以在开机状态下，添加一块 PCMCIA 插槽，或 PC 卡网络适配器，这样不用重新启动计算机，新的局域网络连接图标即可马上添加到文件夹。

可在“属性”菜单选项中配置局域网络连接所使用的网络组件。网络组件指的是客户、服务、以及连接服务器后，与网络服务器联络时所使用的协议。您可配置的组件及其功能如下：

- 服务，例如文件和打印机共享。

- 协议，如传输控制协议/Internet 协议 (TCP/IP)
- 客户，例如 Microsoft 网关和 NetWare 客户服务。

有关局域网连接属性配置的详细信息，请参见 Windows 2000 Professional 帮助。

通过“网络和拨号网络连接”文件夹中的局域网络连接“高级设置”菜单选项，您可以设置多个 LAN 适配器配置。使用该选项，可以修改连接用的各适配器的顺序、与适配器相关联的客户、 服务及协议。

Windows 2000 服务和协议

TCP/IP 是 Windows 2000 所使用的标准网络协议。如果一个客户需要从 NetWare 或 Macintosh 服务器上访问文件及打印资源，Microsoft 将为之提供这些网络连接必需的网络协议或与它们运行环境相兼容的网络协议。比如，NWLink 就是一个兼容协议，它是 Microsoft 执行的 Novell IPX/SPX 协议。

可以在需要访问 Macintosh 资源的客户计算机上安装 Macintosh 服务，它包括 AppleTalk 协议。Macintosh 客户也可以访问运行 TCP/IP 的文件服务器。

Windows 2000 试图按用户在“高级设置”对话框中指定的局域网连接顺序使用网络协议与远程服务器连接。仅安装、启用您所需的协议。比如，如果您只需 TCP/IP，却同时加载了 IPX，这将产生不必要的 IPX 和 SAP 网络通信。

TCP/IP 网络客户

TCP/IP 是最为广泛使用的网络协议之一。使用 TCP/IP 网络的客户将分配到一个 IP 地址，或是由网络管理员分配的静态 IP 地址，或是由主机配置协议 (DHCP) 服务器分配的动态 IP 地址。

Windows 2000 使用一种被称为 DNS 动态更新的新型 DNS 服务。DNS 为使用 DHCP 及静态 IP 地址的客户提供名称空间。

现在， Windows 客户可摒弃使用 WINS 的需要，而转用 DNS 。

在早期的 Windows 网络中，WINS 与 DHCP 配套使用，允许主机在 WINS 数据库中动态注册他们的 NetBIOS 名称和 IP 地址。如果您网络中的任何客户仍在网络上使用 Microsoft Windows NT 工作站、Microsoft® Windows® 95、Microsoft® Windows® 98 或 Microsoft® Windows® 3.1，那么您依然需要 WINS，因为这些客户使用的是 NetBIOS 命名方法。

在网络中使用 Microsoft DNS 有许多好处；DNS:

- 与其它 DNS 服务器，如 Novell NDS 和 UNIX Bind 具有互操作性。
- 与 Active Directory 集成，并且 Active Directory™ 的支持需要 DNS。
- 与 WINS 和 DHCP 等其它网络服务集成。
- 允许客户通过动态注册他们的 DNS 名称和 IP 地址来更新资源记录。
- 支持服务器间的增量区域复制。
- 支持新建资源的记录类型，包括“服务定位器”(SRV) 和“异步传送模式地址”(ATMA) 记录。

在系统上安装 Microsoft TCP/IP 前，应确定客户是否能收到静态或动态 IP 地址。网络主机在使用 DHCP，还是 IP 地址是静态指派的，这一点必须明确。

DHCP

动态主机配置协议 (DHCP) 允许客户自动得到一个IP 地址。这帮助避免在每台计算机上键入数值引起的配置错误。而且，DHCP 有助于防止把已分配的 IP 地址再用于配置网络中的一台新计算机而引起的地址冲突。此外，DHCP 租用更新程序有助于做到自动、高效地为经常需要更新配置的客户（比如频繁更改位置的移动或便携式计算机用户）更改配置。最后，在网络中配置 DHCP 将有助于更为有效地使用、管理本单位的地址空间， 因为那些已不再为设备所使用的地址将重新放

到地址池中，并重新分配给其他的客户。

要启用 DHCP，客户只需在“ TCP/IP 属性 ”属性页中选取“ 自动获取 IP 地址 ”单选按钮，可从“ 局域网络连接 ”图标访问该属性页。如已初步安装了 Windows 95、Windows 98、Windows NT 或 Windows 2000 Professional，则默认启用该选项；因此，如果正使用 DHCP,不必手动设置 IP 配置。

使用 DHCP 的好处如下：

- 客户，如漫游用户，在网络各处旅行时不必手动更改其 IP 设置。不管连接到哪个子网，只要每个子网能够访问 DHCP 服务器，客户都将自动获得一个新的 IP 地址。
- 不必手动配置 DNS 或 WINS 的设置。只要已对 DHCP 服务器进行配置，使其发布 DHCP 客户这些信息，DHCP 服务器将为客户配置这些设置。要在客户端启用这个选项，只需选取“ 自动获取 DNS 服务器地址 ”选项按钮。有关 DNS 和 WINS 的详细信息，请参见本章稍后的“ TCP/IP 网络客户 ”。
- 不会出现地址重复引起的冲突。

有关部署 DHCP 的详细信息，请参见本书中的“ 确定网络连接策略 ”。

静态地址

如果您分配到静态的 IP 地址， 您可得到以下信息。

- 客户安装的每个网络适配器的 IP 地址及子网掩码。
- 默认网关的 IP 地址。
- 客户是否正参加 DNS or WINS。
- 如果客户正参加 DNS，该客户所在的 DNS 域名，以及主 DNS 服务器及备份 DNS 服务器的 IP 地址。
- 如果客户正参加 WINS，主 WINS 服务器和备份 WINS 服务器的 IP 地址。

Active Directory

Windows 2000 支持 Active Directory，但是 Windows 95（和更高版本）以及 Windows NT 4.0 客户需要附加 Active Directory 客户。配置了 Active Directory 的客户可以通过定位域控制器登录到网络。然后 Active Directory 的功能可以使客户受益非浅。这些优点包括：

- 即时访问网络上所有对象的信息。
- 通过登录身份验证及访问控制使用 Active Directory 安全功能。

备注 Windows 95 和 Windows 98 的 Active Directory 客户由一个在 Windows 2000 Server CD-ROM 的“ Clients ”文件夹中的单独升级包提供。

IPX 网络客户

通过使用 NetWare 客户服务或 NetWare 网关服务，Windows 客户可以与 NetWare 服务器交互。

如果网络中有些服务器使用 Novell NetWare 操作系统，Windows 客户可通过 Netware 客户服务直接连接服务器，或可间接连接基于 Windows 2000 的运行 NetWare 网关服务的服务器。

访问 NetWare 资源所需步骤：

1. 安装 NetWare 客户服务。即获许直接连接 NetWare 的资源。安装 NetWare 客户服务时，NetBIOS NWLink 协议被安装。它是 Microsoft 版本的 IPX 协议，支持运行 Windows 2000 Server 的系统与运行 NetWare 4.x 及更早版本的系统的连接。

2. 连接 Novell NetWare 卷。安装了前面列出服务后，可以通过单击桌面上的“我的网络位置”与 NetWare 卷连接。

3. 连接 NetWare 文件及打印资源。在“设置”菜单的“打印机”文件夹中，可以使用“打印机安装向导”在 Windows 95 或更高版本的客户端添加 NetWare 打印机。只需在向导中，用普通的通用命名规则 (UNC) 格式键入打印机名称，即可添加 NetWare 打印机。

NetWare 网关服务

您可在基于 Windows 2000 的服务器上安装 NetWare 网关服务作为网关使用。客户只需用 TCP/IP，不必运行 NWLink，即可连接到 NetWare 资源。服务器运行 NetWare 网关服务和 NWLink 使客户与 NetWare 服务器相连。此服务与 Windows 2000 Server 一并提供。

NetWare 文件和打印服务

此服务是单独的产品，使基于 Windows 2000 的服务器可以直接向 NetWare 服务器及兼容的客户计算机提供文件和打印服务。对 NetWare 客户而言，通过此服务连接的资源就象任何 NetWare 服务器一样，客户可以访问服务器的卷、文件和打印机。对 NetWare 客户无需作任何更改或附加。

NetWare 客户服务

此项服务允许客户计算机直接连接运行 NetWare 2.x、3.x 或 4.x 的 NetWare 服务器上的文件和打印机资源。您可以使用 NetWare 客户服务访问运行 Novell 目录服务或连接库安全的服务器。此项服务与 Windows 95、Windows 98、Windows NT 及 Windows 2000 Professional 一并提供。

Novell 服务器的 Windows 客户

管理员可通过几个途径使客户能使用 Novell 服务器的文件和打印服务。

本章前面部分“IPX 网络客户”曾对安装 Microsoft 的 NetWare 客户服务进行讨论。

备注 NetWare 客户服务只能在 IPX/SPX 协议上运行。必须使用 Novell 客户才能与只运行 TCP/IP 协议的 NetWare 5.0 服务器进行互操作。

在 Novell NetWare 服务器上安装公用 Internet 文件系统附加组件 Windows 2000 Professional 的文件和打印服务使用了公用 Internet 文件系统 (CIFS) 协议。CIFS 是 Microsoft 服务器消息块 (SMB) 协议的增强版本。安装 CIFS 管理单元，使 NetWare 服务器像基于 Windows 2000 的服务器那样对基于 Windows 2000 的客户作出响应。即便网上所有的计算机都运行 IPX，Windows 客户不用任何附加软件也能在访问基于 Windows 2000 的服务器的文件和打印服务。

Novell NetWare 和 Windows 2000 Server 混合环境中的 Windows 客户

如果 Novell 服务器使用的是 NetWare 核心协议，而 Windows 客户使用的是 CIFS（默认通过 Microsoft 网络的 Microsoft 客户），那么即使网络上所有的计算机都运行 IPX，客户仍可能无法访问 Novell 服务器上的文件和打印服务。有几个途径能使 Windows 客户与 NetWare 和基于 Windows 2000 的服务器通讯。

方法 1:安装NetWare 的文件和打印服务 NetWare 的文件和打印服务使基于 Windows 2000 Server 的服务器能对任何客户像 NetWare 服务器一样作出响应。当用户登录到一台运行 Windows 2000 Server 的计算机时，出现的是类似登录 NetWare 3.x Server 的界面。作为 NWLink IPX/SPX 兼容服务的一部分，文件和打印服务使 Windows 2000 Server 使用 NetWare 服务器同样的对话框，模拟成 NetWare 文件和打印服务器。您能用 NetWare 工具来管理 Windows 2000 Server 的文件和打印服务，无须重新培训。而且，使用 NetWare 的文件和打印服务，无需对 NetWare 客户作任何更改。比如，使用 NetWare 协议和命名约定的客户应用程序无需重定向或翻译。

备注 NetWare 文件和打印服务只能用于运行 Windows 2000 Server 及 Windows 2000 Advanced Server 的系统中。

方法 2:安装 NetWare 网关服务 在安装了 NetWare 网关服务后，Windows 2000 Server 就变成了基于 CIFS 的 Windows 客户与 NetWare 服务器通信的网关，允许用户访问该服务器上的所有资源。 运行 Windows 95 及更高版本的客户可使用 TCP/IP，即 Windows 2000 操作系统的网络通信协议，就能访问 NetWare 资源。另外，NetWare 网关服务允许 Windows

2000 网络客户无需 NetWare 客户重定向器或 IPX/SPX协议栈（如 NWLink）即可访问 NetWare 服务器上的文件。这一切，将减少每个客户的管理性负载，从而提高网络的性能。NetWare 网关服务还支持 Novell 目录服务导航、身份验证、打印、及登录脚本。NetWare 网关服务使运行 Windows 2000 Server 的计算机成为 NetWare 网络的通讯网关服务器，重享 NetWare 服务器的网络连接。

打印到 NetWare 打印机

除了传统的打印共享服务外，Windows 2000 Professional 还支持 Novell 分布式打印服务，NetWare 5 的这种增强型打印结构在 Novell 目录服务中集成打印服务。Novell 分布式打印服务还支持双向打印机通信、单座打印机管理，并在打印机首次使用时自动安装正确的打印机驱动程序。

在 NetWare 服务器上配置了 Novell 分布式打印服务的打印机后，按下列步骤安装打印机。

在 NetWare 服务器上安装打印机

1. 在“网络位置”中定位您想安装的打印机。
2. 在打印机图标上单击鼠标右键，然后单击“连接”。
3. 服务器将根据计算机操作系统，安装并配置正确的驱动程序。

NetWare 2.x、3.x、4.x 打印支持 与 Windows 2000 Professional 一并提供。您可直接建立网络打印机连接，或通过映射 LPT 端口或 UNC 端口建立连接。由于 Novell 分布式打印服务要求 Novell 目录服务，因此使用 Novell 分布式打印需要 Novell NetWare 客户。

UNIX 网络客户

计算机需运行相同的协议，才能互相通信。在图 22.2 中，整个网络都运行 TCP/IP 传输协议。在 TCP/IP 层上，UNIX 服务器运行网络文件系统 (NFS) 程序协议（NFS 是 UNIX 文件和打印服务标准），Windows 2000 Server 操作系统运行 CIFS 程序协议。

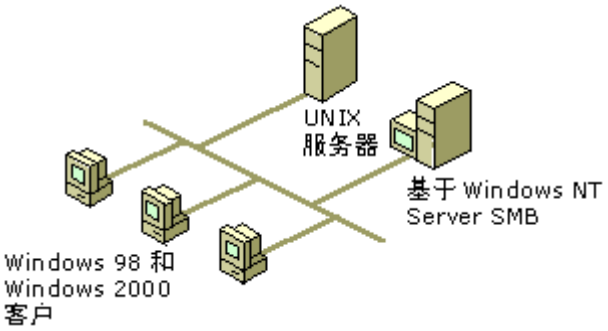


图 22.2 UNIX 和 Windows NT 网络

在通信中，每一种操作系统支持附加功能，如集中管理；远程访问及其它功能；有些已集成到操作系统中，有些可从 Microsoft、UNIX 供应商和独立软件供应商的附加产品得到。

下面是一些集成 UNIX 和基于 Windows 环境的选项概述。

添加 NFS 附加组件到客户 将 NFS 功能（如为 UNIX 的服务提供的）加到桌面系统中，是提供互操作性最普通的一种方法。

添加 CIFS 功能 到 UNIX 服务器 在 UNIX 服务器上安装 CIFS 附件。这使 UNIX 服务器像基于 Windows 2000 的服务器那样对任何基于 Windows 的客户作出响应。

在 Windows 2000 服务器上用 NFS 网关 安装了 NFS 网关产品（UNIX 服务），基于 Windows 2000 的服务器就成了基于 CIFS 的 Windows 客户与 UNIX 服务器通信的网关。用户就能访问 UNIX 服务器上所有的资源，如同它是标准的

Windows 2000 的文件共享。

利用集成的 Telnet 及文件传输协议客户 Windows 2000 服务器提供了 Telnet 及文件传输协议 (FTP) 客户作为操作系统的标准组件。通过这些客户，Windows 2000 Professional 的用户就能与支持 Telnet 协议的任何的 UNIX 系统建立起标准的 VT100 外壳会话，也可使用 FTP 在 UNIX 和 Windows 2000 Professional 系统间传输文件。

AppleTalk 网络客户

可以添加 Macintosh 服务到 Windows 2000 服务器上，这样 Macintosh 系统就能访问这些服务器。一个基于 Windows 2000 Server 的服务器经过这样配置，将出现在 AppleTalk 区域，并且允许用与其它 Macintosh 系统同样的方法去访问。

高级客户连接

用 ATM 为网络媒体、并需要高度连通性的客户可使用 Windows 2000 对异步传输模式(ATM) 及 ATM 上 IP 的支持。有了这些类型的技术，在繁忙的网络环境中，也能确保客户得到最大的带宽。在以下的部分中将讨论这些技术。

异步传输模式

通过连接 ATM 网络，客户们将得到高速及优质服务。在计划客户 ATM 连接策略时，应确定是把客户直接连到 ATM，还是保持现有的以太网结构并使用仿真 LAN (LANE)。如果客户将使用现有的结构，现有的以太网网络硬件已足够了。那么您需要 LANE 把以太网网段连接到 ATM 网络核心。

直接连接的 ATM

在客户使用直接连接的 ATM 之前，需要一个与 Windows 2000 相匹配的 ATM 卡，您可查看“硬件兼容列表”(HCL) 来验证其兼容性。有关 HCL 的详细信息，请参见 Web 资源页的 Microsoft Windows Hardware Compatibility List 链接，地址是： http://windows.microsoft.com/windows2000/reskit/webresources。如果 ATM 网络卡不支持即插即用检测，请与软件供应商联系，获取安装软件。系统检测到 ATM 卡后，将配置仿真 LAN。

IP/ATM

IP/ ATM 使客户能用 TCP/IP 协议高速访问网络。IP/ ATM 网络用 ATM 地址解析协议 (ARP) 服务器把 IP 地址转换成 ATM 地址，并允许访问 ATM 网络上的服务器。多播地址解析协议服务器 (MARS) 能解析多播地址。

红外数据协会协议组

Windows 2000 Professional、Windows 98 及 Windows 95 支持红外数据协会 (IrDA) 的协议组。这个协议，使用户在计算机间无需物理电缆即能传输信息和共享打印机等资源。大多数新的便携式计算机都装有支持 IrDA 的硬件。

例如，两个携带膝上型电脑的用户在旅途中，无需使用电缆或软盘，只需建立 IrDA 连接即可传输文件。只需把便携式计算机放置在近距离内，即可建立 IrDA 连接。IrDA 支持 3 英尺左右的距离。

IrDA 允许访问附加到另一台计算机的资源。比如，如果您想用膝上型电脑打印一个文档，您可以与一台在本地或通过网络连接打印机的计算机建立 IrDA 连接。建立连接后，有适当权限的用户可以通过 IrDA 连接进行打印。有些打印机能直接支持 IrDA，允许用户通过计算机的 IrDA 端口直接向打印机发送打印任务。

Windows 2000 Professional 还能允许或限制非计算机所有者使用 IrDA 来发送文件。用户还可指定接收文档的位置。Windows 2000 Professional 能自动检测使用红外通讯的设备，如其他计算机和照相机。

远程访问客户

使用 Windows 2000 路由和远程访问服务是公司提高其生产力的一个方法。当客户不在本地时，这项服务使他们以最快的速度、最大的安全性远程访问内部网络资源。Windows 2000 Professional 使用户可以通过拨号、红外及直接电缆连接，异常便捷地远程连接网络，包括虚拟专用网络(VPNs)。

“网络连接向导”帮助用户用单一工具建立起新的连接类型。连接建立自动完成，无需下载或安装额外的服务。图 22.3 展示了网络连接向导。

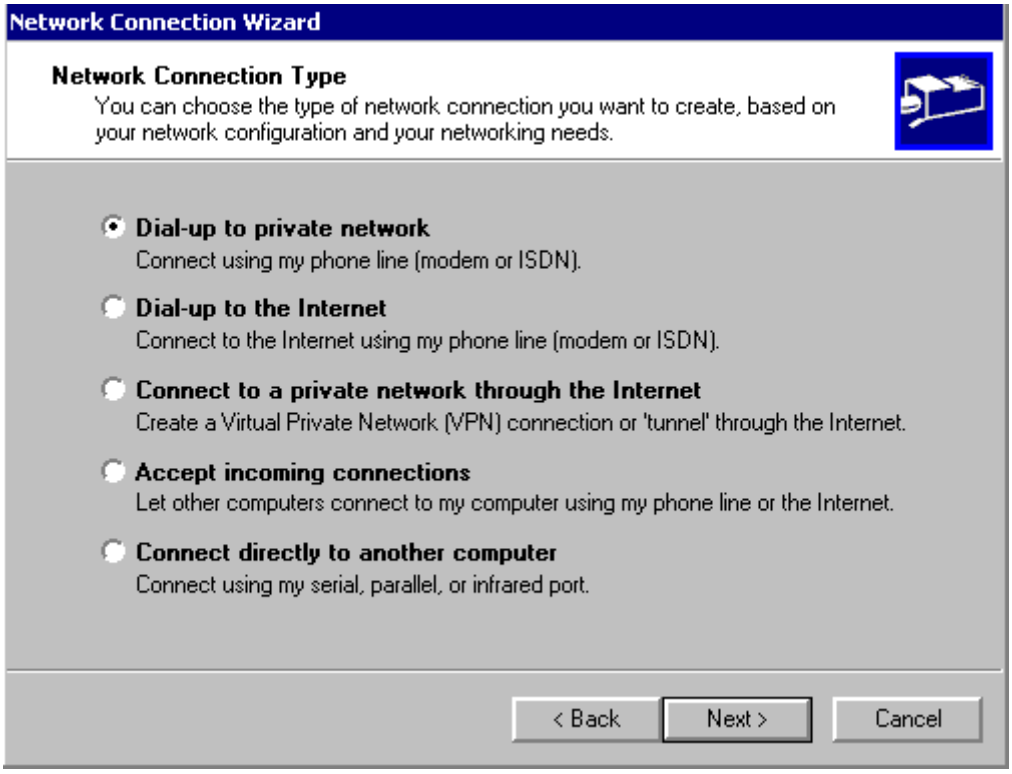


图 22.3 网络连接向导

拨入专用网络

不想使用远程访问专用网络（VPNs）的客户，可以直接拨入企业远程访问服务器来访问这些资源。使用这种方法的优点是您只需拨号连接，而不用通过 Internet 服务提供商（ISP）。使用这种方法的缺点是潜在的长途话费。

虚拟专用网络

当今高级网络的远程客户，能通过 VPN 协议访问各种资源。Windows 2000 除了支持广泛使用的点对点隧道协议（PPTP），也通过使用第二层隧道协议（L2TP），与网际协议安全（IPSec）配套使用，建立起安全的连接。

使用 L2TP 和 IPSec，可以通过远程客户的 ISP 建立起安全通道，使客户在收发数据时不受来自 Internet 的侵扰。

IPSec 是专为两台计算机间传输数据进行加密而设计的，使数据免受网络上未经授权的修改或解释。首先，管理员需定义两台计算机间的互信度，然后指定计算机如何保护它们的通信。一个由管理员在本地计算机上创建及应用、或是使用 Active Directory 组策略的 IPSec 策略中包含该配置。由于 IPSec 策略的配置难度，Microsoft 已经在 L2TP 中内置了 IPSec 支持，这样要做的只是用 L2TP 在远程计算机与 VPN 服务器间建立 VPN 连接。 关于 IPSec 的详细信息，请参见《TCP/IP Core Networking Guide》中的“Internet Protocol Security”。

在交换数据的两台主机上匀应安装 IPSec 管理单元，才能在 Internet 或网络客户上使用 IPSec。如果远程用户通过当地的 Internet 服务提供商（ISP）拨入，该客户及它正拨入的 VPN 服务器匀应运行 IPSec 协议。如果一个内部网的两个客户想安全地交换数据，这两个客户也匀应运行 IPSec。

远程网络连接方法

有多种方法可以部署网络，要根据您正在创建的基础结构而定。可以按其规模分类，它们包括：

- 小办公室/家居办公室网络（SOHO）

- 中大型商业机构使用的中型网络。
- 拥有数千客户的大型企业网络。

小办公室网络

小办公室/家居办公室（SOHO）网络主要用于和所属的较大企业分开的家居办公室。SOHO 使用两种技术，允许 SOHO 客户连接 Internet 或企业网，或两者都能连接。它们分别是 Internet 连接共享（ICS）及网络地址转换（NAT）技术。

SOHO 网络通常为对等网络。这种网络为一个单独的子网，无需路由器、DHCP 服务服务器或 WINS 服务器就可方便地连接客户。如果在一个家居办公室中，用户需要使用不只一台计算机，并且需要与其它计算机共享如文件、程序或打印机等资源，这种网络十分理想。

下面的章节将解释这两种技术的优点、要求及其部署。

SOHO 连接

除了建立并维护一个安全的 Internet 的连接外，SOHO 还应具备管理、组织其内部网络结构的能力。

通过一个“自动专用 IP 寻址”功能，Windows 2000 使 SOHO 能给内部计算机自动分配专用 IP 地址。在连接 Internet 时，您也可给 SOHO 分配地址。这是通过网络地址转换（NAT）做到的。NAT 能把专用 IP 地址转换成用于 Internet 间通信的公用 IP 地址这使得内部的安全不受 Internet 的影响，同时也省下 SOHO 用户获取和维护公用地址范围的时间和费用。图 22.1 说明了实现 SOHO 网络可能需要的因素。

图 22.1 设计小办公室/家居办公室

网络组件	方法
Windows 2000 Server	确保服务器硬件符合 Windows 2000 HCL 所列的规范。
LAN 媒体	使用 10 或 100BaseT 无屏蔽双绞线、10 或 100BaseT 网络集线器或者 10 或 100BaseT 的网络适配器。请参见“HCL 网络适配器兼容要求”。
Internet 连接	使用 ICS、NAT 或路由连接到 Internet.使用 POTS、ISDN、 部分 T1 连接、电缆调制解调器或 DSL。
内部客户连接	使用自动专用 IP 寻址（APIPA)、指定 ISP 或静态 IP 地址。
网络协议	TCP/IP

Internet 连接共享

“Internet 连接共享”是一个包括了 DHCP、网络地址转换（NAT）及 DNS 的简单软件包。可使用 ICS 将您的 SOHO 连接到 Internet，ISC 提供了一个简单的、单步配置允许转换连接，这样允许所有的网络计算机访问电子邮件、Web 及 FTP 站点等。ICS 为 SOHO 网络上所有的计算机提供网络地址转换（请参见下一章节）、自动 IP 寻址及名称解析服务。ICS 提供了下列：

- 单一的复选框，可以轻松配置。
- 单一的公用 IP 地址。
- SOHO 主机固定的地址范围。
- DNS 名称解析代理

- 用于对等网络的单一 SOHO 界面。

使用能启用连接共享的单一复选框，可在新的或已有的远程访问或 LAN 连接上配置 ICS。必须有与当地 ISP 建立了网络连接的计算机、网络界面卡或用于连接对等网络的适配器，才能使用 ICS.与当地 ISP 连接将激活 ICS，并从 ISP 处得到 IP 地址。当 ICS 的连接被激活，网络适配器被自动配置到介于 192.168.0.0 至 192.168.254.254 IP 地址范围之内的 192.168.0.1 这个静态 IP 地址。ICS 系统的计算机也是从这个范围获取 IP 地址。

备注 注意 ICS 被激活后，不允许在网络上再对其它如同 DNS 或 IP 寻址等服务进行配置。这些服务将由 ICS 系统来执行。

网络地址转换

网络地址转换 (NAT) 异于 ICS，功能很类似，但更灵活。也多一些设置步骤。NAT 和 ICS 之间主要的区别在于，NAT 要求至少 Windows 2000 服务器，而 ICS 能在 Windows 2000 Professional 或 Windows 98 第二版中配置。可以在“ Windows 2000 路由和远程访问管理器 ”中加载并配置 NAT。NAT 提供了下列：

手动配置 用户可以用功能更强的方法来配置转换的远程访问连接。

多个公用 IP 地址 NAT 可以使用不只一个公用地址范围。

可配置的地址范围 NAT 允许手动配置 IP 地址和子网掩码，而 ICS 使用固定的 IP 地址范围。使用“ 路由及远程管理 ”中的NAT 属性，可配置任何范围的 IP 地址。DHCP 分配器用与 DHCP 同样的方法提供 IP 地址分配机制。通过在 NAT 属性表中选取“ 使用 DHCP 自动分配 IP 地址 ”复选框，NAT 还可使用由 DHCP 服务器分配的 IP 地址。

DNS 及 WINS 代理 使用 DNS 或 WINS 均可建立名称解析。通过选取“ 名称解析 ”选项卡下 NAT 属性表中的适当复选框，对其进行配置。

多网络界面 通过在“ 路由和远程访问管理器 ”中给 NAT 添加界面，可以就可在把 NAT 功能分配到不止一个网络界面上。

使用 NAT 的网络也可启动使用 PPTP 的 VPN 连接。由此，小型企业、甚至连安装了 NAT 的 SOHO 网络，也能与企业网络建立起安全的远程连接。

备注 由于可能与其它的服务冲突，不要在有其它的 Windows 2000 Server 域控制器、DNS 服务器、网关、DHCP 服务器，或其它为静态 IP 配置的系统的网络上使用 NAT.

不要将 NAT 直接连接到企业网，因为这样　身份验证、IPSec 及 Internet 密钥加密 (IKE) 将不能工作。

自动专用 IP 寻址

在网络中如未能检测到 DHCP 服务器，Windows 2000 Server、Windows 2000 Professional 和 Windows 98 将从 169.254.0.0/16 地址范围中为自己分配一个 IP 地址。Windows 3.11、Windows NT 3.51 和 Windows NT 4.0 也能从这个范围中获取一个 IP 地址，但需从 APIPA 服务器获取。通过运行“ 路由和远程访问管理器 ”，添加并配置 NAT，添加分配 IP 地址的界面，并在 NAT 属性中用前面列举的地址范围重新配置 IP 地址范围，即可设置 APIPA 在这个范围内分配 IP 地址。

有关 APIPA 的详细信息，请参见本书中的“ 确定网络连接策略 ”。

备注 只有 Windows 98 和 Windows 2000 Professional 客户才能参加 APIPA。而其它系统需要一个服务器运行 Windows 2000 路由和远程访问服务，由此服务器向这些系统分配 APIPA 地址。

SOHO 示例

在下列章节中，举两例说明如何应用 SOHO.

例 1

这是个家庭网络的例子，在该 SOHO 上有 5 台计算机。通过 ICS 将 SOHO 与 Internet 连接，然后通过 PPTP 隧道用 Internet 与企业网络连接。客户使用的 IP 地址范围是由 ICS 计算机分配的。如果其中一个客户需要与企业网络相连接，此客户将配置一个 VPN 配置文件，然后开始启用一个通过 Internet 到企业网络的 PPTP 隧道。图 22,4 描绘了这个关系。

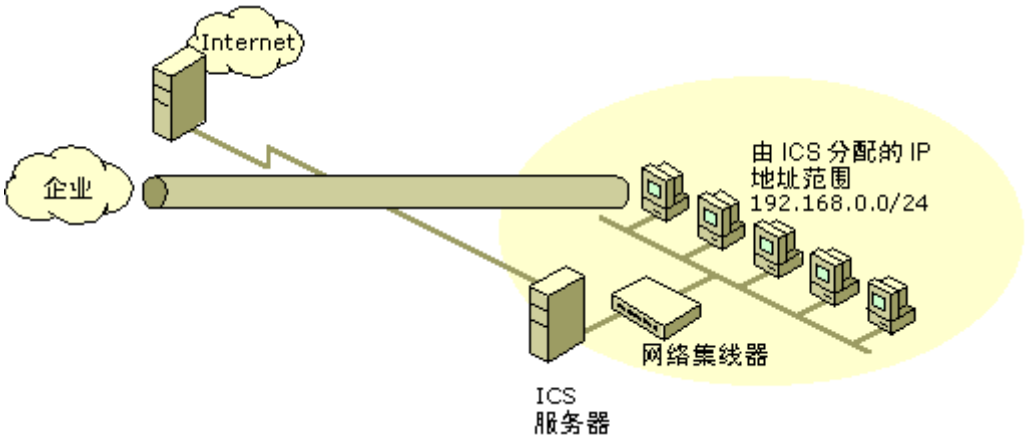


Figure 22.4 家庭网络

例 2

在这个被称为“ strip-mall ”的 SOHO 例子中，客户们通过一个运行着“ 路由及远程访问 ”的服务器进入企业网络。网络客户通过企业网络进入 Internet。图 22.5 描绘了这个网络。

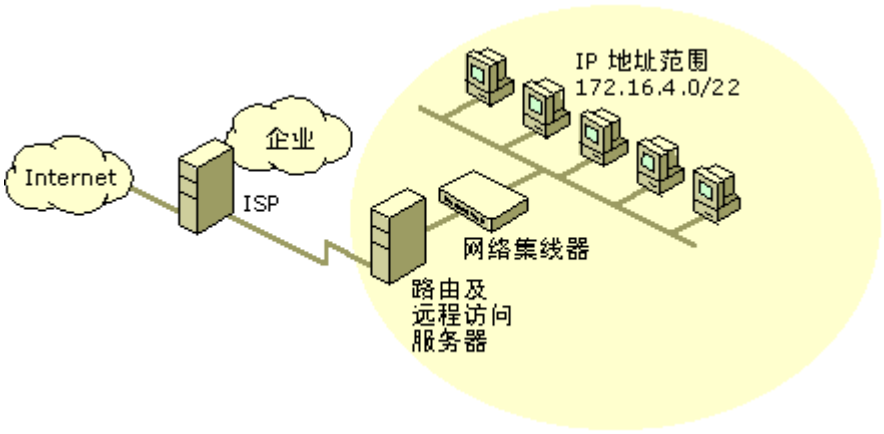


图 22.5 “ Strip-mall ”网络

中大型网络

中大型网络需要一个更有活力的结构，要求一些链接的子网以满足客户需求增加引起网络增长的潜在需要。

路由和远程访问

Windows 2000 路由和远程访问服务，能使企业提高生产力。当客户不在企业内部时，这项服务使他们能远程访问内部网络资源。此项服务也提供了实现最快速度及最大安全性的几个方法。Windows 2000 Professional 让用户通过拨号、红外及直接电缆连接，更便捷地远程连接网络，包括虚拟专用网络 (VPNs)。

“ 网络连接向导 ”帮助用户用单一工具建立起新的连接类型。连接建立自动进行，无需下载或安装额外的服务——而在 Windows 95 中建立某些类型的远程网络时，这一步是必须的。图 22.6 显示了“ 网络连接向导 ”。

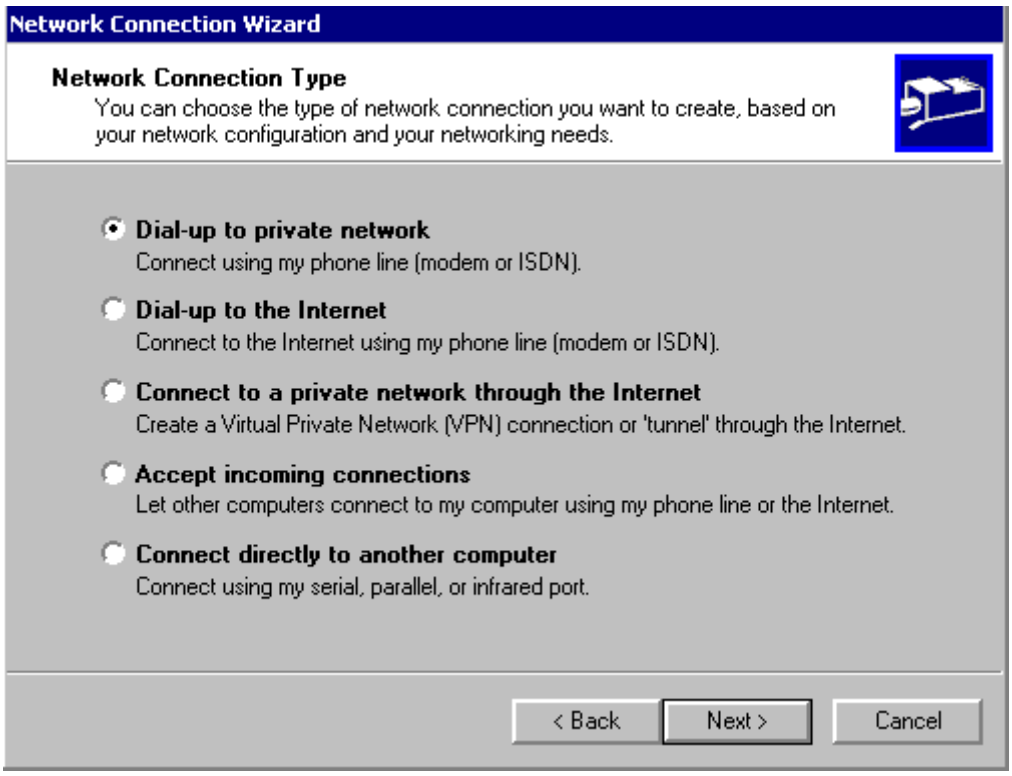


图 22.6 网络连接向导

拨入专用网络

不想远程登录专用网络（VPNs）的客户，可以直接拨入企业远程访问服务器来访问这些资源。唯一的需要是为允许进行用户访问的远程客户设置权限。它的缺点是，用户和公司会面临潜在的长途话费。

直接拨号

客户可直接拨入企业远程访问服务器以传送文件，收发电子邮件。这是一种方便的访问网络的方法，但是很费钱。长途话费，在一段时间之后，会增加远程用户和企业的费用。额外的费用包括管理直接拨号基础设施的费用。在有些情况下，使用 Windows 2000 Internet 身份验证服务（IAS）把直接拨号服务外包出去，或许会更经济些。有关 IAS 的详细信息，参见本书中的“确定网络连接策略”。

为了使客户能连接到企业远程服务器，客户必须得到企业网络相应的权限。您需要选择“控制面板”上“网络和拨号网络”文件夹中的“建立新连接”，在客户计算机上建立拨号配置文件。

客户访问他们的企业帐号的另一种方法是使用 VPN，将在下一章节中讨论这一点。

通过 ISP 使用虚拟专用网络

当今高级网络的远程客户，能通过 VPN 协议访问各种资源。Windows 2000 除了支持 PPTP 外，还通过联合使用 L2TP 与 IPSec 建立十分安全的连接。使用 L2TP 和 IPSec，可以通过远程客户的 ISP 建立安全隧道，使客户在收发数据时不受来自 Internet 的侵扰。

IPSec 是专为两台计算机间传输数据加密而设计的，使数据免受网络上未经授权的修改或解释。首先，管理员需定义两台计算机间的互信度，然后指定计算机如何来保护它们的通信。管理员在本地计算机上创建及应用的 IPSec 策略，或是使用 Active Directory 组策略的 IPSec 策略中包含该配置。由于 IPSec 策略的配置难度，Microsoft 已经在 L2TP 中内置了 IPSec 支持，这样只需用 L2TP 在远程计算机与 VPN 服务器间建立 VPN 连接。 关于 IPSec 的详细信息，请参见《TCP/IP Core Networking Guide》中的“Internet Protocol Security”。

在交换数据的两台主机上匀应安装 IPSec 管理单元，才能在 Internet 或网络客户上使用 IPSec。如果远程用户通过当地的 Internet 服务提供商 (ISP) 拨入，该客户及它正拨入的 VPN 服务器均应运行 IPSec 协议。如果一个内部网络的两个客户想安全地交换数据，这两个客户也均应运行 IPSec。

中大型网络示例

大中型的网络拥有成百上千台的计算机以及多个子网。SOHO 与 Internet 或企业网络连接所用的技术，则需要有更多的配置，但同时也拥有更多的能力。表 22.2 列出了各种技术，以及如何在各类网络中运用它们。

图 22.2 网络技术

SOHO	中型网络	大型网络
使用 ICS，专用 IP 地址范围 192.168.0.0/24.	使用配置了适当的专用 IP 地址范围的 NAT	使用 Microsoft 代理服务器连接到 Internet，并使用 DHCP 分配 IP 地址。
只使用 PPTP。	只使用 PPTP。	用单独的 VPN 服务器来许可 PPTP 和 L2TP/IPSec 隧道。
只使用单一网络界面。	使用多个网络界面。	代理器及 VPN 服务器附加到一个拥有多个网络界面的路由器。
只用 DNS 名称解析。	使用 DNS 或 WINS 名称解析，或两者兼用。	使用 DNS 或 WINS名称解析、或两者兼用。

在规模稍小的 SOHO 网络上，如果只有一个子网及一个 Internet 连接，ICS 表现出色。由于能向多个子网，多个 IP 地址范围提供服务，中型网络可以使用 NAT 把客户连接到 Internet。较大的网络则需要代理服务器以及 VPN 服务器，才能使客户访问 Internet 和隧道通信。

大型网络需要在它们的基础结构有一个称为“ 非军事区 ”(DMZ) 的区域。非军事区 (DMZ) 是一个网络，它在允许 Internet 到专用网络的访问的同时还保持了该网络的安全。任何有暴露于 Internet 界面的服务器集中于此。有关非军事区的详细信息，请参见本书中的“ 确定网络连接策略 ”。

在本例中，一个大中型的企业使用网络为 3 个站点中的 750 至 1,000 名员工提供服务。该网络上的站点使用 T1 和 部分 T1 连接。该企业有一部分远程用户通过拨号接收文件及电子邮件，每个员工都有自己的远程访问帐号。每个站点还有一个 Internet 连接，用于员工因业务需要访问 Internet。该网络正处于从 NetWare 到 Windows 2000 基础结构的过渡期，在 Windows 2000 和 NetWare 共存的环境中客户机和服务器之间的互操作性是必要的。

图 22.7 是此例的一个简化图示。

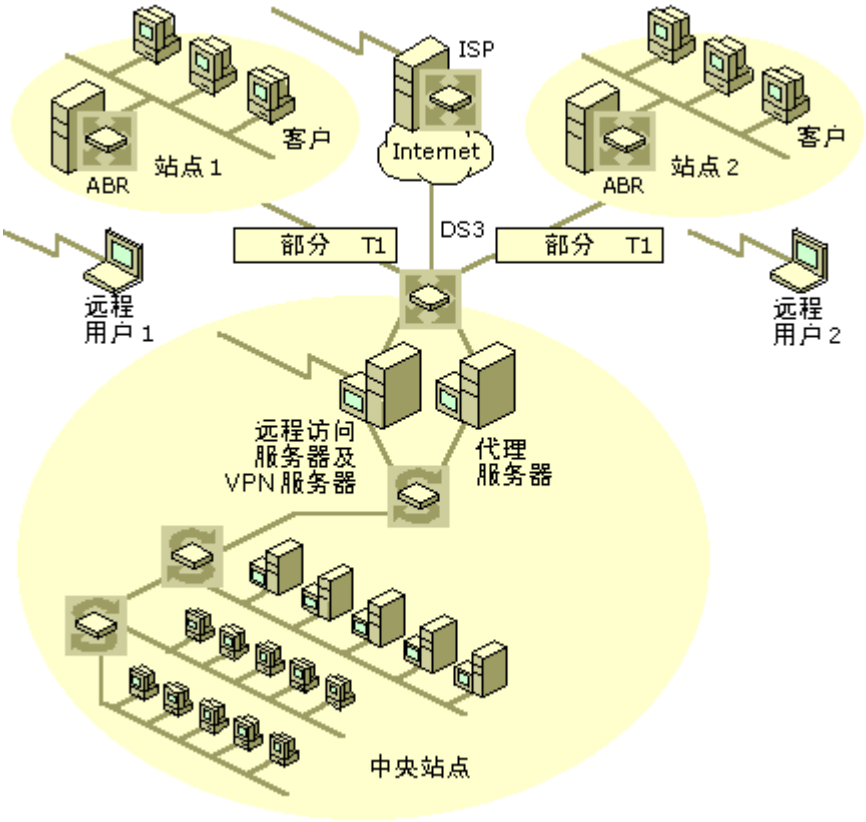


图 22.7 中大型网络

网络客户如下：

- Windows 98 客户
- Windows 2000 Professional 客户
- Windows 95 客户
- Windows NT 4.0 Workstation 客户
- NetWare 客户

由于该网络正缓慢地从 NetWare 过渡到 Windows 2000，大多数员工仍需访问 NetWare 服务器和打印机。一些在仍运行着 IPX 的部分网络上的 Windows 客户正在使用 NetWare 网关服务并运行 NWLink 协议。其他的 Windows 客户正使用 TCP/IP，并通过运行 NetWare 网关服务的 Windows 2000 路由器来访问需要的 NetWare 文件和打印机。远程客户通过多协议 VPN 及位于中央站点内非军事区 (DMZ) 中的远程访问服务器访问基于 Windows 2000 的服务器及 NetWare 服务器。这个网络上的客户从 DHCP 服务器获取他们的 IP 地址，并通过一个位于 DMZ 内的代理服务器访问 Internet。有关中大型网络设计的详细信息，请参见本书中的“确定网络连接策略”。

客户连接规划任务列表

表 22.3 列出了确定网络连接策略时所需完成的任务。

表 22.3 客户连接规划任务列表

任务	章节

确定适当的协议用法。	Windows 2000 服务和协议
配置静态 IP 客户。	静态地址
配置 DHCP 选项。	DHCP
配置使用 IPX 的客户。	IPX 网络客户
配置使用 IPX 的客户。	AppleTalk 网络客户
有关拨号/VPN 访问的决策。	中大型网络

第 23 章 - 定义客户管理与配置标准

提高用户办公效率及降低与管理客户计算机相关的成本是大多数 IT 单位的主要目标之一。Microsoft® Windows® 2000 Server 与 Microsoft® Windows® 2000 Professional 提供了大量面向用户、面向管理的功能，客户和移动计算队伍可运用这些功能提高用户的办公效率，管理客户支持费用。

本章致力于帮助您识别这些功能并在本单位实现这些功能。此外，本章还介绍了由 Windows 2000 Professional 及 Windows 2000 Server 中的组策略提供的扩展的管理功能。此信息将会帮助您创建管理和客户标准，以便运用这些功能的单位使用。如果还没有创建管理和客户标准，请先对您所在单位的客户软件及硬件的基础结构进行评估。有关详细信息，参见本书中的“建立 Windows 2000 测试实验室”和“测试应用程序与 Windows 2000 的兼容性”。此外，可能还需复查您所在单位的 IT 管理目标。

本章内容

使客户系统可管理
使用组策略管理客户
配置硬件
定义用户界面标准
客户标准规划任务列表

本章目标

本章将帮助您创建下列规划文档：

- 客户管理计划
- 首选客户配置

资源工具包中的相关信息

- 有关使用组策略及创建管理模板 (.adm) 文件的详细信息，参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide* 中“组策略”的内容。
- 有关使用 Windows 2000 的 Microsoft® IntelliMirror® 功能的详细信息，参见本书中的“应用更改与配置管理”。
- 有关安装服务和工具的详细信息，参见本书中的“客户自动安装与升级”与“使用 Systems Management Server 部署 Windows 2000”。
- 有关部署终端服务的详细信息，参见本书的“部署终端服务”。
- 有关规划 Windows 2000 安全功能的详细信息，参见本书的“规划分布式安全”。

使客户系统可管理

管理和支持客户计算机既可以是一种简单行为，也可以极端复杂。一般情况下，大单位的用户拥有不同的技术水平。他们使用各种不同的应用程序和硬件，又常常在十分分散的场所中工作。工作时远离站点，及通过低速链接时断时续地连至网络的用户比例逐渐增加。大量研究表明，使用方式各异和客户配置标准的缺乏，是使 IT 支持成本上升的最重要的因素。

本章将帮助您定义基本的客户配置标准，无论用户在何处工作，或其工作要求如何，此标准都能满足他们的需要。此外，还可通过本章内容掌握如何使用组策略来更好地管理基于 Windows 2000 的客户计算机。

规划客户计算机标准既需要技术知识，又需要对单位的了解。必须理解当前的计算机环境，明确所在单位和用户的需要。还须决定要启用 Windows 2000 的哪种功能，然后将满足既定目标所需的更改记录下来。客户计算机标准规划必须说明以下几点：

- 用户及其计算机要求。
- 应用程序及应用程序要求。
- 硬件及硬件要求。
- 当前的及希望的管理模型。
- 重要的支持问题及这些问题的解决方案。

可根据自己的研究，以及对 Windows 2000 Server 和 Windows 2000 Professional 中新的客户支持功能的理解，规划客户管理与配置标准。

图 23.1 是创建客户管理与配置标准的规划过程图解。

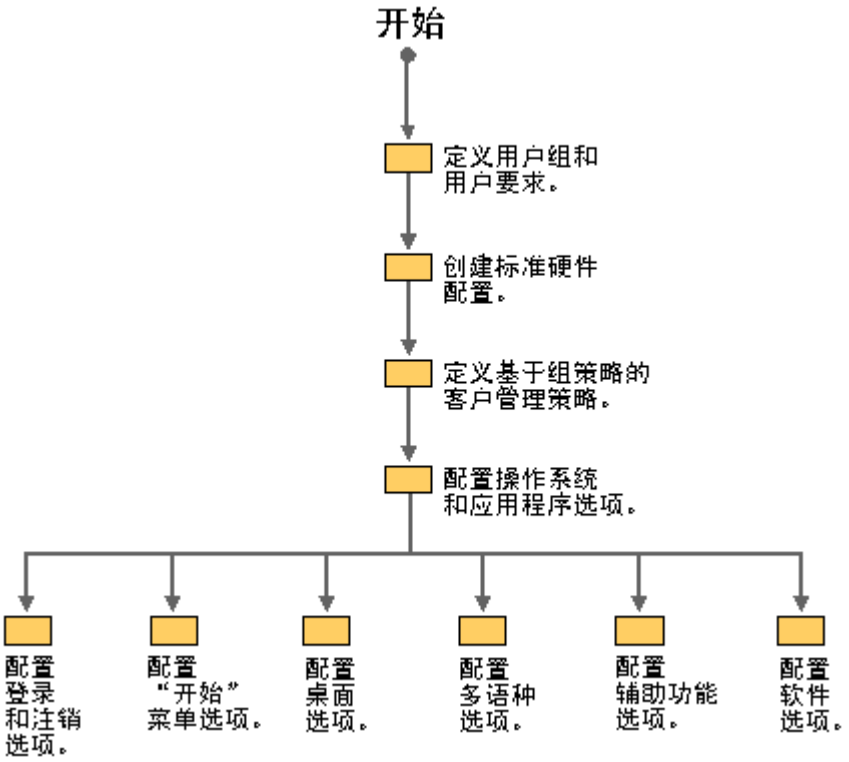


图 23.1 客户管理与配置规划简图

在一个章节中无法涵盖创建客户标准所涉及的众多问题。因此，本章仅讲述以下 Windows 2000 客户管理与配置选项：

- 硬件配置选项。运行 Windows 2000 所需标准的便携式计算机与台式计算机硬件配置选项。
- 管理选项。组策略，指在 Windows 2000 中用于实现客户管理与配置选项的主要方法。

  操作系统与应用程序选项。用户工作时所需的操作系统与应用程序。以及 Windows 2000 中的“开始”菜单和桌面配置选项，包括：

- 多语种选项。在 Windows 2000 自带的多语种计算机支持或新的 Windows 2000 多语种版本中进行选择。

- 辅助功能选项。使需要使用辅助功能的用户能够更便捷地使用计算机的 Windows 2000 功能。

本书的其他章节将会介绍以下 Windows 2000 客户管理与配置选项：

- 在“规划分布式安全”一章介绍客户安全措施选项。
- 支持 Active Directory™ 目录服务的客户管理功能、用户数据管理、软件安装与维护及用户设置管理（通过术语 IntelliMirror 及远程 OS 安装了解），都在“应用更改与配置管理”中加以介绍。
- 在“定义客户连接策略”一章中讨论网络访问。

完成本章所述的规划任务后，可阅读并执行以上所列章节中的规划任务，以完成客户管理与配置标准规划。

定义用户类型

大单位有许多不同类型的用户。下文列出了影响用户的计算机使用方式的一些差异：

- 用户所属的部门（OU）（如财务部、工程部或市场部）。
- 用户执行的工作类型（如技术、行政或管理支持）。
- 用户工作的场所（如在办公室中、远程位置或共享的计算机上）。
- 用户执行其工作所需的自主程度。
- 用户所需支持的量与类型。

此外，还需注意用户是否是：

漫游用户，指许多用户会由一台计算机转移到另一台计算机。当漫游用户由一个场所移至另一个场所时，一般不会随身携带一台计算机；而是使用工作所在地的计算机。接待人员或银行出纳常常在几个不同的办公桌上工作，他们是漫游用户的例子。

移动用户；指有些经常出差的工作人员用便携式计算机工作，目前这种用户逐渐增多。出差时，常常会从网络上断开；这些用户经常会用低带宽连接来连接网络。销售人员和咨询人员常属于移动用户这一类。

远程用户；远程用户与移动用户不同，因为一般情况下，远程用户在固定场所连接至网络，如在单位的分支机构或家庭办公室中，这种连接常常是速度很慢或时断时续。

基于任务的用户；这些用户需要用计算机执行一系列特定的、有一定限制的任务，如输入定单。基于任务的用户可能只需一台运行终端服务的计算机。接待人员和银行出纳是基于任务的用户的实例。

专业工作者；指对计算机提出要求最多的那些用户，例如工程师、律师、图形设计人员及程序员，他们通常需要专业应用程序和自定义的配置。

在执行其他操作前，请先创建一个如表 23.1 所示的表格，用于列出单位内部的用户类型（有些雇员可能属于多个类别）。

表 23.1 用户类型示例表

工作	类别	工作组	位置	所需应用程序	所需支持	自主程度

财务主管	专业工作者	财务部	总部	必需的与可选的	普通	高
部门经理	远程专业工作者	市场部	部门办公室	必需的与可选的	普通	高
销售人员	移动的专业工作者	市场部	变化	必需的与可选的	普通	高
组装工人	基于任务的漫游工作者	生产部	工厂各个车间	必需的	高	低
接待人员	基于任务的漫游工作者	管理部	总部的不同位置	必需的	高	低

要创建客户标准，只靠用户提供的信息是不够的。还必须深入了解用户的需求并考虑他们可能会碰到的问题（例如：由于计算机故障而导致的数据丢失；无论身在何处均可对数据拥有同等的访问权限；或者，即使经常与网络断开连接，其数据仍可与其他用户的数据保持同步）。只有当您真正了解用户及其对计算机的需求后，才会设计出恰当的客户标准。

评估各类型用户的要求

了解用户的基本业务需求后，要完成客户标准还需评估当前环境及所期望的环境。要做到这一点，请检查以下内容：

- 软件要求
- 计算机硬件
- 管理模型
- 桌面配置

下面几节提供了“ 基本 ”和“ 高级 ”用户所需的代表性设置。此处所定义的基本要求通常适用于基于任务的雇员。高级要求一般用于专业工作者。有关如何满足基本用户与高级用户要求的详细信息，参见本书中“ 应用更改与配置管理 ”。但是，这些配置文件均是一般性的。不同单位的标准会有所不同；可能需根据所在单位的要求来创建其他用户类别的标准。

定义软件标准

一般情况下，大单位支持单位内的上千个（有时上万个）不同软件应用程序及软件应用程序的不同版本，包括操作系统。许多单位可通过实现核心软件标准（指整个单位通用的功能，如电子邮件、字处理程序、电子数据表格），以及淘汰过时的和不必要的软件，来降低其客户计算机的成本。

要建立自己的客户应用程序标准，必须注意以下问题，这些问题涉及操作系统、一般商业应用程序，如字处理软件、内部开发的用于执行客户管理或定单填写等任务的业务线应用程序：

- 单位必需的软件有哪些？
- 特定工作或业务部门所必需的软件有哪些？
- 对于单位、业务部门或执行特种工作的工作人员，哪些软件是可选的？
- 单位的软件需求每隔多长时间需要改变？
- 由谁来决定整个单位和特定工作组所用的软件类型？
- 如何自定义软件？
- 如何分发软件？

- 如何配置软件？
- 如何安装新的客户软件？
- 如何升级原有的软件？
- 如何测试或评价新软件？

与此同时，还需决定与 Windows 2000 一起部署哪个软件及如何部署。如果软件未随操作系统一起安装，则可根据需要，让用户能够使用这些软件。

基本用户

基本用户需要操作系统的标准化配置，及最少量的公司标准应用程序，如电子邮件软件、字处理程序，及其工作所需的专用应用程序（例如：定单录入应用程序）。但是，不允许基本用户安装可选的应用程序和较复杂的应用程序功能，如电子表格应用程序的数据透视表格。

高级用户

高级用户常常需要操作系统的高级功能，例如，创建个人网络共享的功能。他们通常还会需要其他可选的应用程序和功能，并可根据需要进行安装。但是，仍可禁止高级用户安装未经批准的应用程序。

备注：在决定哪些应用程序是必需的，哪些是可选的之后，查阅本书的“应用更改与配置管理”、“客户自动安装与升级”及“使用 Systems Management Server 部署 Windows 2000”等内容，以确定如何安装和管理这些应用程序。

定义硬件标准

用户工作所需的应用程序决定公司的硬件要求。但是，规划硬件预算所花费的时间往往超过规划软件升级所用的时间。因而，应仔细规划，以便当用户需要计算机硬件时，应允许用户有充分的时间使用计算机硬件。

以下是有关单位客户的有可能问及的一些问题：

- 当前客户的台式计算机的处理器速度是多少？所用的便携式计算机的处理器速度是多少？
- 当前客户的网络连接速度是多少（包括通过网络连接和调制解调器连接的便携式计算机）？
- 它们的随机存取存储器 (RAM) 的大小及硬盘空间有多大？
- 有无可用于当前网卡及其他外围设备的 Windows 2000 驱动程序？
- 所用的文件系统是什么？
- 是升级当前计算机运行的其他操作系统，还是需要从头开始安装？
- 当前计算机是否可以使用远程启动技术？是否有与远程启动兼容的网卡？是否可以使用远程启动软盘？
- 是否会用网络共享来存储用户数据和配置数据？
- 由谁负责备份用户数据？

- 如何将新计算机在单位投入运行？如何部署新硬件？原设备制造商是否预先安装了应用程序？是否删除新硬件的预先安装软件，而后根据自己的标准重新安装？
- 如何替换出故障的硬件？如何替换出故障的硬盘？如何替换或还原操作系统？如何替换或还原应用程序？如何替换或还原用户数据？
- 硬盘上的数据是否有安全要求？是否使用任何形式的数据加密？
- 计算机是否有多种配置？例如，便携式计算机在插接站（包括网卡）中使用一套硬件功能；而当其不在插接站（用高速调制解调器而非网卡）时，则使用另一个硬件配置文件？
- 在替换计算机、还原标准操作系统和应用程序环境之前，用多长时间来排除硬件故障？

针对单位中每一类用户，定义一种能够满足目前及预期处理要求（至少两年内）的计算机标准类型。此外，还应尽量减少支持的不同硬件配置的数量，以提高对用户的支持能力，降低客户支持成本。

有关升级和从头安装选项的详细信息，参见本书中的“客户自动安装与升级”和“使用 Systems Management Server 部署 Windows 2000”。有关远程 OS 安装及脱机文件夹的详细信息，参见本书的“应用更改与配置管理”一章。

因为大多数单位不能为所有雇员都购买最新的、功能强大的全能型计算机，所以，在表 23.1 中，指导方针示例说明如何根据用户组的需要来配备计算机硬件。

表 23.2 计算机分配策略示例

如果计算机	将其分配给：	还需考虑：
不能满足 Windows 2000 对硬件的最低要求	基于任务的用户	在此硬件中使用终端服务
满足 Windows 2000 对硬件的最低要求	基本用户（包括漫游用户和基于任务的用户）	为基本用户提供永久性网络连接
超过 Windows 2000 对硬件的最低要求	高级用户（包括专业的和移动的工作人员）	

定义重要支持问题

了解目前存在的支持问题将有助于改善客户管理与配置标准，并能降低支持成本。下列问题将帮助您确定哪些管理策略能为单位提供最有价值的功能。

- 最严重的十个支持问题是什么？

  列出这些问题，并设计行动方案来降低其发生频率。

- 每隔多长时间用户会因试着更改设置（如显卡驱动程序）和其他配置选项而“破坏”其配置？

  如果发生配置问题的频率高得让人无法接受，则会希望限制用户更改其操作系统配置的权限。

- 每隔多长时间会因用户不正确地添加或删除应用程序而“破坏”了配置？

  如果此问题的发生频率高得让人无法接受，则会希望限制用户安装或卸载应用程序的权限。

- 用户是否在其计算机上安装未经授权的软件？

如果单位中存在此问题，则须着手制订企业策略，确定是否允许使用未经授权的软件。即使允许用户将未经授权的软件带入单位，仍需定义允许用户使用的软件类型及其必须遵守的授权规则。

- 客户机上的数据是否有安全措施？这些数据是否需要安全措施？

  大多数单位会希望为企业数据定义安全措施。涉及的数据类型不同，其相应的安全级别也会有所不同（例如，财务数据或贸易机密需要一个安全级别，而公共关系发布的有关数据则需要另一个安全级别）。此外，您可能还想根据数据类型，定义由谁负责数据的安全（例如，由 IT 还是由用户）。

- 是否允许用户以本地管理员的身份操作计算机？

  如果用户过去曾获准作为本地管理员操作，那么，安装新操作系统则是调整其权限的理想时机：此时可更改或微调其权限，使其更有效地满足单位管理的需要。

- 帮助中心重新安装或重新设置基本配置之前，花费多长时间来修复损坏的配置？

  如果对损坏配置的支持调用没有时间限制，则应考虑为其设定限制条件。同时，还应评估 Windows 2000 的可用于备份用户数据、安装或重新安装操作系统和应用程序的一些功能。这些新功能会影响支持调用的长度。例如，如果与排除受损坏配置的故障相比，重新安装桌面和数据更方便，则可以大大降低支持调用的平均长度。

解答上述及其他支持问题将帮助您确定实现哪些 Windows 2000 功能和配置选项。在本章稍后的内容中，将讨论多种代表性配置和控制选项。

解答这些与支持相关的问题还会帮助您评估当前管理模型和标准的效率。改进后的管理模型常常会弥补客户服务中存在的差距与不足。下节将帮助您评估现有的管理模型。

定义管理模型和标准

到目前为止，由于无法以最佳方式委派单位的 IT 管理任务，IT 经理的工作受到了很大限制。有鉴于此，Windows 2000 提供了经过显著改进的支持，用来控制客户和委派管理任务。

您的 IT 管理模型是否反映了所在单位的当前结构？如果您的 IT 管理模型已经过时，则需要重新评估所有主要的 IT 任务及其执行位置，以便能够更有效地委派和执行这些任务。需要回答的问题包括：

- 由谁创建或更改用户帐户或计算机帐户？每个月要创建或修改多少用户帐户或计算机帐户？

  在许多发展迅速的单位中，仅靠一个人或一组已无法及时更新用户或计算机信息。或者，合并后的单位或并购的单位可能是由多人或多个组，以冗余的方式来执行彼此类似的任务。因此，您需要确定委派这些 IT 任务的最有效方式：是在域层次、部门层次还是在站点层次。

- 由谁建立软件标准？由谁负责部署软件？

  如果单位尚无软件标准，那么，迁移至新操作系统则是建立一个标准的理想时机，有了这些标准，即可使用户更有效地交流和共享信息。您还会发现许多分部或部门有其独特的应用程序要求。那么定义应用程序标准时，既要适应单位的集中要求，又要适应其分散的要求。

- 由谁设置或更新密码？密码或身份验证的要求是什么？

许多单位将重新设置密码的权限委派给帮助中心。或者，密码要求自身可能在在单位的较高级别进行确定，且常常是一套身份验证要求应用于整个单位。

- 由谁备份服务器？由谁备份用户数据?每隔多长时间进行一次备份？每隔多长时间由备份还原一次数据？

  许多单位只备份服务器，而通常由用户备份自己的数据（但用户很少这样做，甚至根本不备份）。如果单位没有提供用户数据的备份，则应考虑为用户建立服务器共享，并要求用户将重要的数据存储于这些共享，以便能够定期执行备份。

- 所在单位是否有服务等级协议或其他明确的服务目标？所在单位明确的服务目标或成功的标准是什么？

  越来越多的单位正准备设立明确的服务目标或签署服务等级协议，使其为达成量化结果而负责。您的 Windows 2000 客户管理计划中应包括现有的或新建的服务目标。设立明确的目标有助于改进客户管理计划，克服其存在的缺点，使其能够满足单位的要求。

总结管理和配置目标

在进行下一步的工作之前，请先总结所在单位现有的客户支持计划及希望采纳的支持标准。

同时，还应总结单位现有的客户管理模型，以及希望用 Windows 2000 提供的功能和性能来实现的管理模型。

使用组策略管理客户

如何使用组策略来管理客户取决于所设置的服务标准及目标。

在管理水平较高的环境中，服务等级协议应包括：提供快速疑难解答（例如，在十五分钟内响应）指南、出现故障时快速进行设备替换，及经常备份数据（可能每天一次）。此外，管理水平高的支持还应包括一些高级功能，例如：基于组策略的用户或计算机环境；软件安装与维护；脱机文件夹；以及用于登录、注销、启动和关闭进程的自定义脚本。

在管理水平低的环境中，支持和设备替换所花时间可能会较长；并且此环境所提供的服务只是管理水平高的环境所提供服务的一部分。

而在不受管理环境中，用户为自己提供疑难解答、自己替换设备、备份数据，并运用的基于组策略的功能最少。

后面的章节阐述了使用 Microsoft® Windows NT® version 4.0 系统策略、Windows 2000 Professional 本地组策略以及基于 Windows 2000 Active Directory 的组策略所能提供的支持的级别和质量。运用此知识，即可在单位的最有效层次中，委派对关键客户支持任务的控制权。

比较 Windows NT 4.0 系统策略与 Windows 2000 组策略

Microsoft 在 Windows NT 4.0 中引入了系统策略编辑器，用于指定存储于 Windows NT 注册表的用户配置和计算机配置。使用系统策略编辑器，就可以创建系统策略，用来控制用户工作环境、为所有运行 Windows NT 4.0 Workstation 或 Windows NT 4.0 Server 的计算机实施系统配置的设置。

在 Windows NT 4.0 (及 Microsoft® Windows® 95 和 Microsoft® Windows® 98) 中有 72 种策略设置。这些设置：

- 仅根据 .adm 文件设置注册表项目值。
- 应用于域。
- 由安全组中的用户成员进一步控制。
- 不安全。
- 只要未撤消指定策略，或者用户未编辑注册表，就会一直保存在用户配置文件中。
- 主要用于锁定桌面。
- 只可用 .adm 文件扩展。

在 Windows 2000 中，组策略设置是管理员启用集中更改和配置管理的主要方法。可用组策略为某个特定的用户组和计算机组创建指定的桌面配置。要自定义组策略来实现这一目标，可用 Microsoft 管理控制台 (MMC) 组策略管理单元。组策略管理单元将替换 Windows NT 4.0 系统策略编辑器，并使您能够更好地控制计算机组和用户组的设置。

Windows 2000 组策略有 100 多种与安全有关的设置和 450 多种基于注册表的设置，为您管理用户计算机环境提供了众多选项。Windows 2000 组策略：

- 可根据 Active Directory 或在本地进行定义。
- 可用 Microsoft 管理控制台 (MMC) 或 .adm 文件扩展。
- 是安全的。
- 不会在实施的策略改变时把设置留在用户配置文件中。
- 可应用于指定的 Active Directory 容器（站点、域与 OU）中的用户或计算机。
- 可由安全组的用户或计算机成员进一步控制。
- 可用来配置多种类型的安全设置。（有关安全设置的详细信息，参见本书的“规划分布式安全”一章。）
- 可用于实施登录、注销、启动及关闭脚本。
- 可用于安装和维护软件。
- 可用于重定向文件夹（如 My Documents 和 Application Data 文件夹）。
- 可用于在 Microsoft® Internet Explorer 中执行维护。

创建的组策略设置包含于组策略对象中，这些对象与所选的 Active Directory 站点、域及 OU 相链接。组策略用以文档为中心的方法来创建、存储和关联策略设置。组策略把设置存储于组策略对象中，这与 Microsoft® Word 将信息存储于 .doc 文件类似。

此外，可通过使用安全组来筛选组策略对象，以精确调整单位的组策略在计算机及用户中的使用。这保证了对组策略的处理更加快捷。

将 Windows NT 4.0 策略应用于 Windows 2000

如果把基于 Windows NT 4.0 的客户机和服务器变成基于 Windows 2000，则会改变策略的执行方式。应根据用户帐户对象和计算机帐户对象的位置，即是在基于 Windows NT 4.0 Server 的服务器中，还是位于基于 Windows 2000 Server、带有 Active Directory 的服务器中，来确定您的迁移策略。表 23.3 假设存在一个基于 Windows 2000 的客户。所有接受 Windows NT 4.0 系统策略的客户均是通过用户登录服务器中的 Netlogon 共享来获取这些策略的。

表 23.3 服务器操作系统的预期行为

环境	帐户对象的位置	影响客户的因素
纯粹的 Windows NT 4.0	计算机：Windows NT 4.0	**计算机启动时**：计算机本地组策略（只有更改时）。 **每当用户登录时：**计算机系统策略。
	计算机刷新	**按 Control-Alt-Delete 前：**只有计算机本地组策略。 **用户登录后：**计算机本地组策略和计算机系统策略。
	用户：Windows NT 4.0	**用户登录时：**用户系统策略。 **如果本地组策略更改：**用户本地组策略与用户系统策略。
	用户刷新	用户本地组策略与用户系统策略。
混合（迁移）	计算机：Windows NT 4.0	**计算机启动时**：计算机本地组策略（只有更改时）。 **每当用户登录时**：计算机系统策略。
	计算机刷新	**按 Control-Alt-Delete 前：**只有计算机本地组策略。 **用户登录后：**计算机本地组策略和计算机系统策略。
	用户：Windows 2000	**用户登录时：**处理计算机系统策略后再处理组策略。
	用户刷新	用户组策略。
混合（迁移）	计算机：Windows 2000	**系统启动期间：**组策略。
	计算机刷新	计算机组策略
	用户：Windows NT 4.0	用户登录时：用户系统策略。 **如果本地组策略更改**：用户本地组策略与用户系统策略。
	用户刷新	用户本地组策略与用户系统策略。
Windows 2000	计算机：Windows 2000	**计算机启动期间和用户登录时：**组策略。
	用户：Windows 2000	
无 Active Directory	本地	只有本地组策略。

备注：当计算机帐户对象位于 Windows NT 4.0 域中，而用户帐户对象位于 Windows 2000 域时，则会在用户登录时处理计算机系统策略。可用 NTConfig.pol 文件来执行此操作，该文件位于基于 Windows 2000 的、用来验证用户的域控制器（而非基于 Windows NT 4.0 的域控制器）的 Netlogon 共享中。但建议您移出这种混合处理模式，而尽快改为纯粹的 Windows 2000 模式。

没有可用于修改此行为的选项。要简化单位中的管理，请考虑尽快用 Windows 2000 组策略替换 Windows NT 4.0 系统策略。

使用 Active Directory 委派客户管理

如果环境中包括 Windows 2000 Professional、Windows 2000 Server、以及 Active Directory 名称空间，则在此环境中启用的 Windows 2000 客户管理是最完整的。

组策略设置与一个 Active Directory 容器（域、站点或 OU）关联。您所配置的组策略设置与单位的 Active Directory 结构相结合，使您可按照需要将客户标准定义得很宽（适用于整个单位）或很窄（仅适用于一个工作组、一种工作职能或一个工作场所的成员）。实施组策略设置的层次需要对照单位的管理模型进行校准，该模型与 Active Directory 和域模型一同定义。

虽然承担过创建和实施客户标准任务的 IT 小组不参与规划域名空间的工作，但如果所在单位正在规划 Active Directory 名称空间，则强烈建议您规划域名空间。因为在规划过程中，域名空间小组了解您的客户管理要求和目标越早，单位最终的名称空间设计就越有可能提高您管理和支持用户要求的能力。

注意：如果尚未开发 Active Directory 名称空间，则需客户管理小组与目录和名称空间小组合作，以便在单位的最有效层次中设置客户标准、定义组策略设置和执行管理任务。

设计良好的 Active Directory 名称空间可以相对简化在域或 OU 层次实现某种客户标准（如企业的电子邮件）。这还为委派管理能力提供了方便，委派后即可在其他层次管理指定的客户任务，例如添加或删除用户、修改桌面配置或执行工作组应用程序。

例如，您可能想为整个企业定义域层次的安全和基本应用程序（如电子邮件、字处理）标准。但是，如果可授予站点或 OU 层次的管理助手有限的权力，使其能够执行添加和删除用户的操作，那么若再让企业级管理员来执行这些例行的频繁更改，则会导致工作效率低下。

与此类似，当需要新密码时，如果通常最先呼叫的是站点或 OU 级的帮助中心成员，那么，域级管理员则并非重新设置密码的最佳人选。使用 Windows 2000 组策略，可以把与密码相关的任务委派给帮助中心人员，又不必授予其访问某些设置的权限（这些设置是不希望他们进行更改的）。

作为客户管理规划的组成部分：

- 识别所有与客户相关的管理任务，例如：新计算机的设置；用户帐户的设置、传送与删除；软件安装与升级；疑难解答；客户配置标准的定义。
- 识别目前正在单位的什么位置执行这些任务。
- 识别需在单位的哪个层次来执行这些任务。

有关组策略与 Active Directory 结构之间关系的详细信息，参见本书的“设计 Active Directory 结构”一章。

委派组策略的管理

部署 Active Directory 的单位还可委派对部分目录服务的控制权，因此也能委派本章上文所述的一些客户管理任务的职责。本节介绍了组策略允许您委派站点、域和 OU 层次中管理任务的方法。

由组策略委派管理涉及下列三个任务，可按情况的需要同时或分别执行它们：

- 管理站点、域或 OU 的组策略链接。
- 创建组策略对象。

- 编辑组策略对象。

管理站点、域或 OU 的组策略链接

默认情况下，只有域管理员组和企业管理员组可以配置站点、域或部门的组策略。可在站点、域或 OU 的“ 属性 ”页的“ 组策略 ”选项卡中指定链接至站点、域或 OU 的组策略对象。

Active Directory 支持以每个属性为基础的安全设置。这意味着您可授予非管理员读/写指定属性的权限。在这种情况下，如果已委派非管理员执行“ 管理组策略链接 ”的任务，他们就能够管理链接至该站点、域或 OU 的组策略对象。要使用户具有此种能力，请使用委派向导。

创建组策略对象

默认情况下，只有域管理员组、企业管理员组和组策略创建者（所有者）组的成员可以创建新的组策略对象。如果域管理员想使一个非管理员或一个组能够创建组策略对象，则可将该用户或组添至组策略创建者（所有者）安全组中。这样，非管理员作为组策略创建者（所有者）组的成员，当其创建组策略对象时，就成为组策略对象的创建者和所有者，并可编辑此对象。但即使非管理员隶属于组策略创建者（所有者）组，也只对他所创建的或明确委派给他的组策略对象拥有完整的控制权。

编辑组策略对象

默认情况下，组策略对象接受域管理员、企业管理员及组策略创建者（所有者）组成员的完全控制，但不需要应用组策略属性的设置。这意味着，虽然这些成员可编辑组策略对象，但该组策略对象中所含的策略却无法应用于这些成员。

默认情况下，已验证的用户对含应用组策略属性设置的组策略对象拥有读的访问权限。这意味着组策略会影响这些用户。

因为域管理员和企业管理员也是已验证用户的成员，所以默认情况下，只要未明确将其排除，这些组的成员就会受组策略对象的影响。

当一个非管理员创建了一个组策略对象时，此人即成为这个组策略对象的创建者（所有者）。当管理员创建组策略对象时，域管理员组即成为这个组策略对象的创建者（所有者）。

要编辑组策略对象，用户必须对该组策略对象同时拥有读和写的访问权限。要编辑组策略对象，用户必须是以下成员之一：

- 隶属于域管理员组或企业管理员组。
- 隶属于组策略创建者（所有者）组，并且必须在此之前已创建过组策略对象。
- 对组策略对象拥有委派的访问权限的用户。即这样的管理员或用户：他/她拥有由某个具有恰当权限的人用“ 组策略对象属性 ”页的“ 安全 ”选项卡委派给他/她的访问权限。

创建组策略 MMC 控制台来委派组策略

委派组策略的方法是：先创建并保存组策略管理单元控制台（.msc 文件），然后指定哪些用户和组对组策略对象或 Active Directory 容器拥有访问权限。可用组策略对象“ 属性 ”页的“ 安全 ”选项卡来定义组策略对象的权限；这些权限会授予或剥夺指定的组对组策略对象的访问权限。

可用于 MMC 的策略设置增强了此种类型的委派。有的策略可用于“ 管理模板 ”节点，此节点位于“ Microsoft 管理控制台 ”的“ Windows 组件 ”中。这些策略使管理员能够定义受影响用户可能会运行或不会运行哪些 MMC 管理单元。策略定义既可以是包容性的，即只允许运行一套管理单元；也可以是排他性的，即不允许运行一套管理单元。

特殊组策略实现选项

如果能认真应用组策略选项，即使开始用数据极其多的文件夹重定向选项和软件安装选项，也能够改善网络的响应时间。应恰当地应用组策略选项，尤其在刚开始时，更要仔细测试所有建议的更改，以确保不损坏网络性能。

此外，许多实施选项允许您无须创建额外的组策略对象，即可微调组策略的应用程序。下面是一些可用的选项：

- 安全组筛选选项
- 不许替代（强制）组策略对象选项
- 阻止 OU 策略继承的选项
- 处理“环回”策略设置的策略选项
- 低速链接处理的选项
- 周期刷新选项
- 同步和异步处理的选项

下面几节简短介绍了以上各种选项。

安全组筛选选项

通过使用 Windows 2000 安全组，可筛选某个特定组策略对象会影响哪些计算机和用户组。这意味着您可筛选任何组策略对象对指定安全组成员所施加的影响。要执行此操作，请使用组策略对象“属性”页的“安全”选项卡。

例如，可根据恰当的用户自主程度，把不同的用户类型分配给 Windows 2000 用户组。Windows 2000 提供了以下默认的用户组，这些用户组与 Microsoft® Windows NT® version 3.51 和 Windows NT 4.0 的默认组相似，但并不相同：

- Administrators。可完全管理计算机或域的成员。
- Backup Operators。可跳过文件的安全设置备份文件的成员。
- Power Users。这类成员可以修改计算机及安装程序，但不能阅读属于其他用户的文件。还可共享目录和打印机。
- Users。这类成员可以创建和保存文档，但未经管理员许可，既不能安装程序，也不能对系统文件和系统设置进行可能有破坏性的更改。
- Guests。获准对计算机或域进行短时间访问的成员。此类可能包括适用于供应商或承包商的特殊权限。例如，默认情况下禁用 Guest 帐户。

备注：与 Windows NT 4.0 相比，Windows 2000 允许管理员对用户拥有更精确的控制。因而，曾在 Windows NT 3.51 和 4.0 中用于 Users 的默认权限现在应用于 Power Users。而曾在 Windows NT 3.51 和 4.0 中用于 Restricted Users 的默认权限现在则应用于 Users。

在表 23.1 中，财务主管、分部经理及销售人员可能会添至 Power Users 组，接待人员和工厂各车间工作人员会添至 Users 组。也可根据成员执行的任务、其拥有的可修改自己或其他计算机的权限级别、及希望这些成员拥有的配置来创建其他组。例如，您可根据单位内的部门（销售部、人力资源部、工程部等）来细分 Users 组，这样可为所有执行相同任务的雇员创建和部署适当的标准配置。将其用于有不同配置和权限要求的用户，可大大简化管理过程。

要防止把组策略对象策略设置应用于某个指定的组，则需删除该组中的“ 应用组策略访问控制 ”项目。

对于包含非管理员的组，还必须删除“ 读访问权控制 ”项目；因为任何具有读访问权的人均可查看数据。

有关设置及使用安全组的详细信息，参见本书的“ 规划分布式安全 ”一章。

不许替代（强制）和阻止策略选项

指存在这样的选项：选项允许您实施包含在指定的组策略对象中的设置，这样可防止较低层次的 Active Directory 容器中的组策略对象替代该策略。例如，如果在域层次定义了一个指定的组策略对象，并已指定组对象是强制的（不许替代），那么组策略对象所包含的策略设置就会应用于该域中的所有 OU；层次较低的容器（OU）将无法替代此域的组策略。

还可阻止从父 Active Directory 容器继承组策略。例如，如果为一个 OU 指定了“ 阻止策略继承 ”，则会禁止其应用在更高层次 Active Directory 容器（如更高级别的 OU 或域）中指定的组策略对象。但是，不许替代（强制）策略选项始终比阻止策略选项优先。

环回选项

可根据用户或计算机对象在 Active Directory 中所处的位置，对用户或计算机应用组策略。但有时必须要根据计算机对象的物理位置，对用户应用组策略；此位置与用户对象在单位内的逻辑位置不同，例如，在图书馆中，或者一个 OU 的用户登录到另一个 OU 的计算机上。组策略的环回功能使管理员能够根据用户所登录的计算机来应用用户组策略设置。

例如，若应用程序已分配或发行到市场部门（OU）的用户，如果您不希望当用户登录到服务器 OU 时安装这些应用程序，就可以设置环回选项。可用组策略环回支持功能来指定两种其他方式，为服务器 OU 中的任何计算机用户检索组策略对象列表。

合并模式 合并模式中，正常情况下是在登录过程中，用 GetGPOList 应用程序编程接口（API）功能来处理用户的组策略对象列表，然后，在 Active Directory 中使用计算机位置时，会再次调用 GetGPOList API 功能。接着，计算机的组策略对象列表会添至用户组策略对象的结尾。这使计算机的组策略对象比用户的组策略对象更有优先权。

替换模式 此模式中，不处理应用于用户的组策略对象。而只会使用基于计算机对象的组策略对象。

该策略设置的路径是：Computer Configuration\Administrative Templates\System\Group Policy。策略名称是：用户组策略环回处理模式。

低速链接处理

许多用户，如使用便携式计算机的用户、远离建筑物或在分部工作的用户，有时会用低速连接连接至网络。可对许多组策略设置进行配置，使其只在有适当的网络连接时才运行。这些组策略设置包括：

- 软件安装与维护
- 脚本
- 磁盘配额
- IP 安全
- Dfs 故障恢复策略
- Internet Explorer 维护

低速链接策略设置的路径是：Computer Configuration\Administrative Templates\System\Group Policy。所列的每个组策略选项均有一个处理策略，该策略允许您更改低速链接的行为。

当组策略检测低速链接时，将会应用以下的默认设置，除非这些设置被修改：

- 安全设置：开（且无法关闭）。
- 管理模板：开（且无法关闭）。
- 软件安装与维护：关闭。
- 脚本：关闭。
- 文件夹重定向：关闭。
- Internet Explorer 维护：关闭。

除管理模板与安全设置管理单元外，会为其他所有选项提供一个策略，用于切换设置的开关状态。有关配置带低速连接的计算机的详细信息，参见本章稍后的“使用组策略进行配置控制”的内容。

周期刷新处理

可指定定时地处理组策略。默认情况下，每 90 分钟处理一次，并带有 30 分钟的随机偏移量。偏移量是添至刷新间隔的随机时间，用来防止所有客户在同一时间请求组策略。它专门用于阻止不必要的网络峰值负载，例如，当大批用户打开其计算机并在同一时间登录后的 90 分钟，即需要偏移量。可根据需要改变此刷新频率，例如，在测试或演示环境中使用较短的时间间隔；而如果需要，则也可使用较长的时间间隔。

允许您改变刷新频率的策略设置有两种，位于：Computer Configuration\Administrative Templates\System\Group Policy。其中，一个策略设置用于域控制器；另一个用于所有其他计算机（包括其他服务器）。这些策略设置命名为“用于 OU 的组策略刷新间隔”。

同步和异步处理

默认情况下，计算机与用户策略设置的组策略处理都是同步的。在计算机处理过程中，只有当所有计算机组策略设置更新后，用户才能登录。在用户处理过程中，只有当所有用户组策略设置更新后，用户才能访问桌面。这些处理规则提供了最安全的操作模式。

有种组策略设置能够异步处理计算机与用户组策略处理进程。此设置可指示系统在登录提示（计算机设置）或桌面（用户设置）显示之前继续执行操作，而无须等到组策略更新完成。

异步处理的结果是，在应用所有组策略设置之前，可能很快就会显示登录对话框，或者显示准备就绪的 Windows 界面。

如果您指定异步处理，而用户可在计算机或用户设置被处理完之前完成登录过程并开始工作，那么，则有可能为用户带来了很大的问题。例如，如果用户用一个正在修改的应用程序开始工作，那么，处理可能会失败；或者，当计算机和用户设置处理完后，用户可能会遇到意外事件。

使用客户端扩展

有些组策略组件包括客户端扩展（.dlls），这些扩展用于在客户计算机上实施组策略。

当客户处理策略时，可根据需要加载客户端扩展。客户首先会得到一个组策略对象列表。接着，会遍历所有的客户端扩展，以确定每个客户端扩展是否有数据在任意组策略对象中。如果

一个组策略对象中有客户端扩展的数据，那么，调用客户端扩展时，也调用扩展需要处理的组策略列表。如果客户端扩展在任何组策略对象中都没有设置，则不会调用此扩展。

每个组策略客户端扩展均存在一种计算机策略设置。每个策略最多包括三个选项（复选框）。有的客户端扩展只包括两个计算机策略选项，因为第三个选项不适于此扩展。

下节将会解释客户端组策略处理选项。

允许通过低速网络连接处理

当客户端扩展在操作系统中注册时，它会在注册表中设置项目值，用于指定通过低速链接应用策略时，是否必须调用该扩展。有些扩展（如软件安装与维护）要移动大量数据，因此通过低速链接处理可能会影响性能（试想，要通过每秒 28.8 千字节的调制解调器线路来安装一个大型应用程序，将会花费多长时间）。

管理员能够设置视为低速链接的连接速度。此外，如果管理员决定无论数据量多大，均需通过低速链接来运行客户端扩展，他或她即可起用该策略。通向此策略的路径是：Computer Configuration\Administrative Templates\System\Group Policy。

定期的后台处理期间不应用

启动时会应用计算机策略，而后大约每隔 90 分钟会在后台再次应用。用户登录时会应用用户策略，而后大约每隔 90 分钟会在后台再次应用。

因为在后台处理策略是很危险的，所以有些扩展只在初始运行期间处理。例如，对于软件安装和维护，只有在计算机启动或用户登录过程中处理这种应用程序更改才是安全的。否则，正在使用应用程序的用户可能要在工作的同时，卸载应用程序并安装其新版本。

有些扩展允许更改其默认行为。“ 定期的后台处理期间不应用 ”选项可用于替换此默认行为，并可指定扩展是否在后台运行。

即使组策略对象未更改时仍进行处理

默认情况下，只要服务器上的组策略对象还未更改过，就不必不断地将其重新应用于客户，因为客户已拥有全部设置。但如果用户是计算机的管理员，则可以更改策略设置。此时，则需要在登录过程中或定期的刷新周期中重新应用这些设置，以使计算机返回所需的状态。

例如，假设已用组策略来定义一套文件指定的安全选项。后来有管理特权的用户登录并改变该选项。此时，您也许要设置策略，使其即使在组策略对象未更改时仍处理组策略；这样，就会在每次启动或登录时均重新应用安全设置。 也可用于应用程序。组策略可安装一个应用程序，但最终用户却能够删除此应用程序或其图标。“ 即使组策略对象未更改时仍进行处理 ”选项使管理员能够在下次用户登录时强制性还原应用程序。

比较独立和基于 Active Directory 管理功能

在表 23.4 中，总结了有 Active Directory 的 Windows 2000 Professional 或无 Active Directory 的 Windows 2000 Professional 所具有的管理功能。

表 23.4 Windows 2000 Professional 与基于 Active Directory 的管理功能对比

管理功能	Windows 2000 Professional	带 Windows 2000 Server、Active Directory 和组策略的 Windows 2000 Professional
管理模板（基于注册表设置）	X	X

安全设置	X	X
软件安装与维护（指派和发行）	--	X
远程安装	--	X
无人参与安装	X	X
Sysprep	X	X
脚本	X	X
文件夹重定向	--	X
Internet Explorer 维护	X	X
用户配置文件	X	X
漫游用户配置文件	--	X

当组策略主要针对 Active Directory 容器时，也可使用在本地计算机上使用的所有组策略管理单元。

但是，以下活动需要 Windows 2000 Server、一个 Active Directory 基础结构及一个运行 Windows 2000 的客户机：

- 软件安装与维护；即为用户组和计算机组集中管理软件的能力。
- 用户数据与设置管理，包括允许将特殊文件夹重新定向到网络上的文件夹重定向。
- 远程操作系统安装。

有关更改和配置选项的详细信息，参见本书中的“ 应用更改与配置管理 ”一章。

如果最初使用本地组策略，后来又让计算机隶属于一个带 Active Directory、实施组策略的域，则会先处理本地组策略，再处理基于域的组策略。如果域策略与本地组策略之间存在冲突，则会先处理域策略。但是如果后来计算机离开了域，则会重新应用本地组策略。

	关键决定 如果在升级为 Windows 2000 Server 之前，把客户升级为 Windows 2000 Professional，而后来又希望转换为受管理的 Active Directory 环境，就必须仔细规划组策略的实施策略，以使用户在更严格的控制完备前不能更改其计算机。例如，如果把 Windows 2000 Professional 部署在不受管理的环境中，后来又要将这些计算机移至受管理的 Active Directory 域，则可能需要重新安装操作系统和应用程序，以确保系统配置尚未遭到未经授权的更改。

在独立计算机上使用组策略

虽不推荐在独立的计算机上部署组策略，但有时候也需要这样做。

在一台独立的计算机上运行 Windows 2000 Professional 时，本地组策略对象位于：\%*SystemRoot*%\System32\GroupPolicy 中。如果组策略管理单元针对本地计算机，则可用下列设置：

- 安全设置。可以只为本地计算机而不为域或网络定义安全设置。

- 管理模板，允许设置 450 多个操作系统行为。
- 脚本。可用脚本自动执行计算机的启动与关闭，还可用脚本来决定用户登录和注销的方法。

以下是一些可通过本地组策略实施的业务规则举例：

- 本计算机的用户不能使用“运行”命令。
- 每当本计算机重新启动时均运行防病毒程序。
- 隐藏“开始”菜单中的公用程序组。

要管理本地计算机的组策略，需要对这些计算机拥有管理权。可按以下步骤来访问用于本地计算机的组策略管理单元：

要访问组策略管理单元

1. 在“开始”菜单中，先单击“运行”，键入 **MMC**，再单击“确定”。
2. 在 MMC 窗口的“控制台”菜单中，单击“添加/删除管理单元”。
3. 在“独立”选项卡上，单击“添加”。
4. 在“添加管理单元”对话框中，单击“组策略”，然后单击“添加”。
5. 当显示“选择组策略对象”对话框时，单击“本地计算机”来编辑本地组策略对象。
6. 单击“完成”。
7. 单击“关闭”。
8. 最后，单击“确定”。组策略管理单元及其针对的本地组策略对象会打开。

此步骤还允许在远程计算机上打开组策略管理单元。在步骤 5 中，单击“浏览”，然后选择所需的计算机。

备注：本地组策略不允许执行安全筛选或同时拥有组策略对象的多个设置（如基于 Active Directory 的组策略对象那样）。但是，可设置文件夹 %SystemRoot%\System32\GroupPolicy 中的任意访问控制列表 (DACL)，这样，本地组策略对象所含的设置即会根据该列表，影响或不影响指定的组。如果计算机是在没有连接到 LAN 的环境（如 kiosk 环境）中使用，那么当需要控制或管理这些计算机时，此选项将会非常有用。与通过 Active Directory 管理的组策略不同，此选项仅用“读”属性；这使得本地组策略可以只影响普通用户而不影响本地管理员。本地管理员可以先设置所需的策略设置，然后将 DACL 设置到本地组策略对象目录，这样作为一个组的管理员就不再具有读的访问权限。如果管理员后来要对本地组策略对象进行更改，他或她就必须先取得目录的所有权，使其本人获得读权限，而后进行修改，修改后再删除其读权限。

配置硬件

迄今为止，您应该了解自己的桌面、工作站、便携式计算机及外围设备中哪些符合 Windows 2000 的最小要求。

	关键决定 在更新系统之前，请先验证当前的基本输入输出系统（BIOS）是否支持 Windows 2000，或验证是否可随时升级与 Windows 2000 兼容的 BIOS。

验证了系统符合 Windows 2000 要求后，就会在安装过程中自动执行大多数 Windows 2000 下的硬件配置工作。但是，下面列出了在客户配置规划中必须指出的、与主要硬件的配置相关的一些问题。

文件系统支持

Microsoft 推荐您用 NTFS 文件系统格式化全部 Windows 2000 分区，这些分区不需要那些运行其他操作系统的客户访问。当系统发生故障时，NTFS 用其日志文件和检查点信息来还原文件系统的一致性。此外，NTFS：

- 支持所有的 Windows 2000 操作系统功能。
- 文件压缩与解压缩改进。
- 可通过将查找文件所需的磁盘访问数量缩减到最低，使访问速度大大加快。
- 文件和文件夹安全得到改善。

在 NTFS 卷，可用组策略指派下列文件权限选项：无权限，列表，读，添加，添加和读，更改，完全控制，特殊目录访问权限，以及特殊文件访问权限。也可用组策略指定哪些用户与组可以访问这些卷，以及允许什么级别的访问权限。

与 Windows 95 及 Windows NT 4.0 Workstation 相比，这些额外的文件安全选项允许单位配置更严格的文件访问权限。如果用户在便携式计算机上存储了敏感信息，他们可将这些文件和文件夹加密。如果便携式计算机被窃，即使窃贼重新安装 Windows 2000 Professional，Windows 2000 加密文件系统（EFS）也会保护其文件和文件夹。但是，请确保管理员及最终用户对加密的文件和文件夹拥有足够的访问权限。

硬件配置文件

如前所述，大多数硬件配置工作是自动执行的。但是，有些型号较早的便携式计算机可能会在插接站与独立使用之间频繁切换，或者，会由主要网络连接转成脱机状态，而后又通过第二种、第三种、甚至第四种不同类型的网络连接重新连接至网络，此时可能会需要一些高级配置。

因为许多便携式计算机的用户在技术上并不精通硬件配置文件的配置，所以，您可能要为这些不同环境配置硬件配置文件，或培训这些用户学会自己修改计算机，以连接至网络。参见图 23.2 的示例。

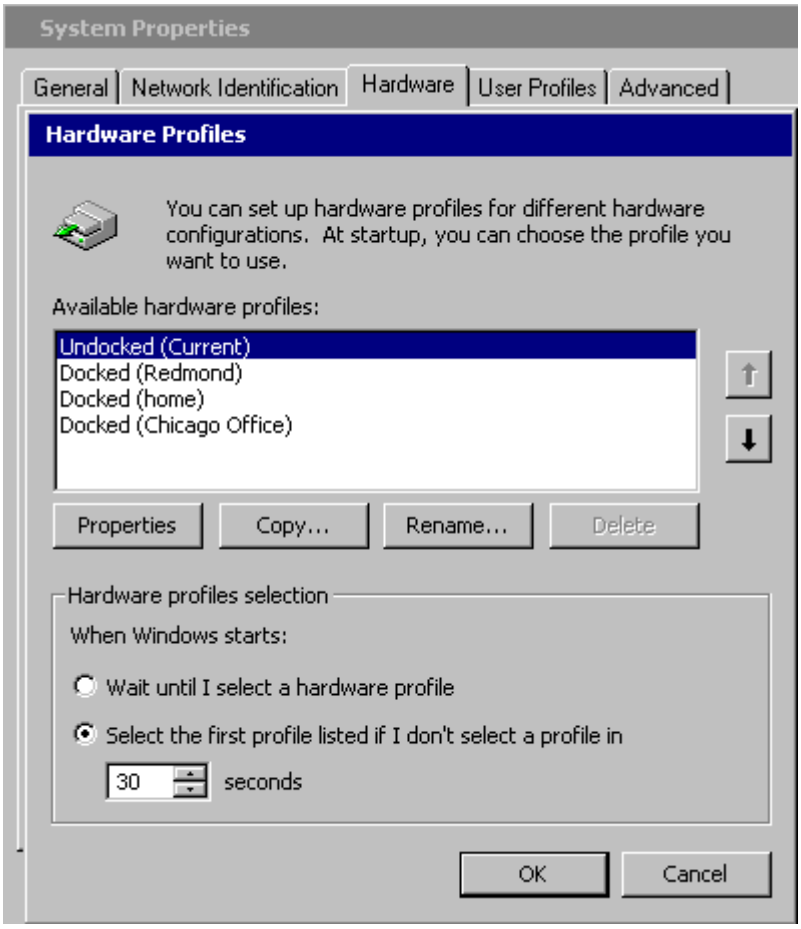


图 23.2 包含多个硬件配置文件的便携式计算机

只有当便携式计算机、配置选项及外围设备都完全相同时，才可为多台计算机同时配置硬件配置文件。或者，可能既想配置一些硬件设置，又想提供额外的最终用户配置培训，使这些用户可以自己执行一些任务。

定义用户界面标准

正如本章上文所述，每个单位都有其特殊的用户计算机要求。Windows 2000 允许您根据所在单位的需要，创建包括用户界面 (UI) 标准在内的标准操作环境。

无论您是接受 Windows 2000 默认值，还是实现自己的 UI 首选项，Microsoft 都推荐您根据以下标准评估 Windows 2000 配置选项：

- 是否易于掌握？
- 使用是否有效？
- 是否易于记忆？
- 是否能有助于指出帮助中心最严重的问题或关注的事宜？
- 是否能减少用户出错的次数？

虽然一般单位不需要象软件制造商（如 Microsoft）那样，如此深入地研究这些问题，但以下技术可能会帮助您配置 Windows 2000，使其更符合用户的要求：

- 集中组。将用户组聚集在一起，集中讨论用户对其计算机配置的意见，即喜欢或不喜欢什么、如何更改才会提高其效率。
- 观察性研究。当用户用计算机工作时，对其进行观察。
- 野外研究。与其他单位的管理员讨论他们所掌握的知识。
- 专家观点。学习与用户界面设计和用户效率有关的已有的研究成果。

下面几节阐述了 Windows 2000 中的许多 UI 选项，您可用组策略配置这些选项。管理员未设置的配置选项成为用户配置文件的一部分，可随意对其进行配置。如果后来创建的组策略会影响配置选项，则组策略拥有优先权。组策略设置始终比由用户实现的 UI 配置有优先权，这些配置保存于用户配置文件中。

基本用户

基本用户比高级用户的计算机经验少；因而，IT 将这些用户的系统配置成效率最高，而其对系统进行可能有害更改的余地最小。因为禁止其使用“ 运行 ”菜单和“ 控制面板 ”，所以只实现管理员用组策略指定的更改。这种用户只可使用管理员分配的网络链接。他们也不能添加或删除未经管理员批准的应用程序。

高级用户

高级用户通常更有经验，常常会运行需要特殊配置选项的要求较高的应用程序，或者会经常断开与网络的连接；因而，应允许这种用户有更多的自由来管理自己的系统。而且，他们还必须能够使用相同的必要登录/注销选项与功能，如多语种与辅助功能选项。

使用组策略进行配置控制

可用组策略控制许多桌面设置和配置选项，例如：

- 自定义登录与注销过程
- 自定义桌面
- 自定义操作系统的多个组件

下面的章节将会阐述每个类别的配置选项。还包括一些代表性示例及不够详尽的列表。切记，有 550 多种不同的组策略设置，查看所有不同选项的最好方法是研究 Windows 2000 的已安装版本。有关组策略设置的详细信息，参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide* 中有关“ 组策略 ”的内容。

当您阅读完本章的其余内容，随后使用 Windows 2000 时，请注意对所在单位有用的选项。然后，可在完成列表后开始自定义符合要求的组策略对象。在您的客户配置规划中，还应包括选项和组策略设置的完整列表。

自定义登录和注销过程

Windows 2000 提供了许多自定义登录和注销过程的方法。例如，可指定每当用户登录或注销时，都运行诊断程序或防病毒程序。

表 23.5 列出了一些可能有用的登录和注销选项。

表 23.5 登录与注销组策略选项示例

策略	说明
运行隐藏的传统登录脚本	默认情况下，Windows 2000 会在命令窗口中显示为 Windows NT 4.0 及其早期版本所编写的运行时的登录脚本指令（不显示为 Windows 2000 编写的登录脚本）。启用此策略可禁止显示为 Windows NT 4.0 或早期版本编写的登录脚本。
将“注销”添至“开始”菜单	将“注销<*用户名*>”添至“开始”菜单，并防止用户将其删除。
退出时不保存设置	在用户的最后一次会话中，回退其对桌面的更改。
登录时不显示欢迎页	隐藏每当用户登录时在 Windows 2000 Professional 中都会显示的欢迎页“Windows 2000 入门”。

限制对桌面的更改

组策略可帮助您防止用户对其计算机进行可能会降低效率的更改。此外，还能使您优化桌面，以适应在单位中执行的特殊任务。表 23.6 列举了一些可用来自定义桌面的策略。

备注：许多单位会希望创建 Internet 和 Intranet 浏览器软件的自定义配置。有关自定义和管理 Internet Explorer 5 的详细信息，参见 Web 资源页的 Microsoft® Internet Explorer Administration Kit (IEAK) 链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources。Windows 2000 包括一个组策略管理单元，称为 Internet Explorer 维护，用于配置和管理 Internet Explorer 5。

表 23.6 自定义桌面选项示例

策略	说明
禁止用户更改 My Documents 的路径	防止用户更改通往“My Documents”文件夹的路径。
禁用控制面板	禁止使用所有控制面板程序。
隐藏“从软盘或光盘添加程序”选项	删除“添加新程序”页中的“从软盘或光盘添加程序”选项。
隐藏指定的控制面板程序	隐藏指定的控制面板项目和文件夹。
禁止改动活动桌面	通过防止用户启用或禁用活动桌面，或防止其更改活动桌面的配置，来实施标准桌面。
活动桌面墙纸	可指定在所有用户的桌面上显示的桌面背景墙纸。
2000 年的世纪解释	指定将两位数年解释为 21 世纪的最后一年的年份。
隐藏“我的电脑”中的指定驱动器	从“我的电脑”、“Windows 资源管理器”及“我的网络位置”中删除代表所选硬盘驱动器的图标。此时，在“打开”对话框中不显示代表所选驱动器的驱动器号。
桌面屏幕保护程序可执行的名称	指定计算机所用的屏幕保护程序。
禁用命令提示	防止用户运行交互式的命令提示，即 Cmd.exe。该策略还决定是否能在计算机上运行批处理文件。
禁用注册表编辑工具	禁止使用 Windows 注册表编辑器 Regedt32.exe 和 Regedit.exe。

限制更改“开始”菜单

在单位中，您可能想对启用哪些“ 开始 ”菜单功能拥有控制权。组策略允许您禁用那些不希望他人使用的选项，还允许您创建优化的“ 开始 ”菜单，使其能够反映单位及用户的需要。表 23.7 列出了几个示例。

表 23.7 代表性的“ 开始 ”菜单选项

策略	说明
禁用并删除到“ Windows Update ”的链接	删除“ Windows Update ”的超级链接。此策略可删除“ 开始 ”菜单中和 Internet Explorer 的“ 工具 ”菜单中的“ Windows Update ”超级链接。
删除“ 开始 ”菜单中的“ 运行 ”命令	删除“ 开始 ”菜单中的“ 运行 ”命令；删除“ 任务管理器 ”中的“ 新任务（运行...） ”命令。同时，有扩展键盘的用户不再能使用“ 运行 ”命令的键盘快捷键显示“ 运行 ”对话框。
将“ 注销 ”添至“ 开始 ”菜单	将“ 注销<*用户名*> ”添至“ 开始 ”菜单，并防止用户将其删除。
在“ 开始 ”菜单中禁用拖放快捷方式菜单	可防止用户用拖放方法重新排列或删除“ 开始 ”菜单中的项目。同时，也可删除“ 开始 ”菜单中的快捷方式菜单。
解析壳快捷方式时，不使用以搜索为基础的方法	防止系统为解析快捷方式，对目标驱动器实施综合搜索。
不运行指定的基于 Windows 的应用程序	防止 Windows 运行您在该策略中指定的程序。

备注：自定义的和提供给用户的“ 开始 ”菜单可存储在本地，或者存储在网络服务器中。

远程用户的配置选项

许多单位中，使用便携式计算机的用户正逐渐增加，使得管理这些远程计算机成为一个引人关注的重要管理问题。表 23.8 的策略可用于管理远程访问用户的用户数据。

表 23.8 便携式和远程计算机选项

策略	说明
限制组策略的使用	即使通过低速链接也无法关闭组策略。（应用限制过分严格的组策略设置，或将大量数据下载到便携式计算机或用户家庭计算机时，请谨慎从事。应考虑到登录脚本和默认的 600 秒超时。）
自动检测低速网络连接	允许为视为低速链接的链接设置阈值。然后，可定义某种消耗带宽的活动，这些活动在遇到低速链接时不会发生。
指定脱机时始终可用的网络文件和文件夹	允许您指定可在脱机时使用的网络文件和文件夹。
禁用“ 可脱机使用 ”	防止用户将某些文件或文件夹改为可用。

添加多语种选项

与以往相比，越来越多的单位正进入地理区域全新的市场，而且还有许多操不同语言的用户在各地旅行。几乎每个国家和地区的中型或大型单位中都存在多语种用户。

这给 IT 管理员带来了一些新的问题，如下所述：

- 须支持操多种语言的用户，以及这样的用户：他们使用计算机时，以一种更方便、效率更高的语言工作，而不是用本地办公室中通常使用的工作语言。需将键盘布局、排序、日期格式、货币格式、帮助文件及类似的本地化设置都必须配置成能够保证最佳效率。

- 因为要为每种可能的语言组合配置操作系统，所以，既给部署增加了不必要的复杂性和成本，又提高支持成本。如果存在多个版本的操作系统，帮助中心的人员就无法轻松地排除故障，纠正错误。

- 如果单位有操作系统的多个本地化版本，那么每次使用时，均须测试或部署相同数量的 Service Pack。

通过使用 Unicode 字符编码、国家语言支持 (NLS) 应用程序编程接口 (API)、多语种 API 及 Windows 资源文件，Windows 2000 增强了对国际化和多语种计算机的支持。无论使用的是 Windows 2000 的 24 个本地化版本中的哪一种，这种多语种技术均使 Windows 2000 能够支持在 100 多个国际场所中所用语言的输入和显示。

此外，Microsoft 提供了一个独立的 Windows 2000 多语种版本，它允许根据不同的用户来改变用户界面语言，从而扩展了 Windows 2000 的本机语言支持。

备注：Windows 2000 多语种版本仅可用于 Microsoft Open License 程序、Select 和 Enterprise 协议客户。有关这些程序的详细信息，参见 Web 资源页的“Licensing Programs for Enterprises”链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources 。

多语种版本允许管理员：

- 将通过网络部署的 Windows 2000 Server 和 Windows 2000 Professional 安装软件包的数量减到最少。

- 支持旅行用户，使其能够使用与所拜访的远程办公室不同的语言。

- 执行管理任务时使用一种语言；而要用不同的语言、相同的计算机、键盘和显示器执行其他任务时，则无须重新启动计算机，即可实现。

- 在运行 Windows 2000 Server 和 Windows 2000 Professional 的计算机中按需要添加或删除多种用户界面语言。

多语种版本不会改变应用程序中使用的语言，而只是改变 Windows 2000 菜单、对话框和帮助文件所用的语言。Microsoft® Office® 2000 多语种包与此类似，它允许许多单位简化 Office 2000 部署选项。

选择多语种版本的注意事项

Windows 2000 多语种版本为国际用户和多语种用户提供了多种选项。表 23.9 帮助您选择适用于所在单位的语言选项。

表 23.9 不同版本的多语种功能及优点

功能	单语种版本	多语种版本
供用户使用的多语种功能	完全本地化的用户界面，包括菜单、帮助文件、对话框及文件夹名称。用户可用 60 多种语言进行输入、查看和打印。	用户可将用户界面切换成自己喜欢的语言。用户也可用 60 多种语言进行输入、查看和打印。
供 IT 专业人员使用的多语种功能	如果并非迫切需要在环境中支持一个以上的语言版本，则该版本对您比较合适。用户仍可查看和编辑其他语言的文档。	如果要在环境中部署和支持一种以上的语言，则该版本对您比较合适。例如，当要部署一个 Service Pack 时，则只需要一个版本。要在一台计算机上支持操多种语言的用户，则该版本对您比较合适。

升级为 Windows 2000 多语种版本

可以只是由 Windows 的国际英语版升级为多语种版本。如果要用 Windows 2000 多语种版本替换 Windows 的其他任何语言版本，则需要从头安装多语种版本。

在规划升级到多语种版本时，要注意一些额外的版本限制。表 23.10 提供了版本兼容指南。

表 23.10 多语种版本升级选项

	Windows 2000 Professional 多语种版本	Windows 2000 Server 多语种版本	Windows 2000 Advanced Server 多语种版本
Windows 3.x	--	--	--
Windows for Workgroups	--	--	--
Windows NT 3.51 Workstation	X	--	--
Windows NT 4,0 Workstation	X	--	--
Windows 95	X	--	--
Windows 98	X	--	--
Windows 2000 Professional	X	--	--
Windows NT 3.51 Server	--	X	X
Windows NT 4,0 Server	--	X	X
Windows 2000 Server	--	X	--
Windows NT 4.0 Terminal Server	--	X	X
Windows NT 4.0 Enterprise Edition	--	--	X
Windows 2000 Advanced Server	--	--	X

规划 Windows 2000 多语种版本安装

仔细考虑下列规划注意事项，这将有助于您更成功地部署 Windows 2000 多语种版本：

- 需要多语种版本的哪些文件和语言组？
- 这些文件需要多大磁盘空间？
- 最好使用哪种安装过程？
- 如何部署这些文件？
- 是从光盘安装还是通过网络共享安装？

多语种版本文件和语言组

在 Windows 2000 多语种版本中，用户界面的语言支持需要两个不同的语言文件集合。

- 语言组包含所有必需字体，以及处理和显示某种语言组所必需的其他文件。

- 多语种版本文件，可为 UI 和帮助系统提供语言内容。

根据您所安装的每种 UI 语言，Windows 2000 多语种版本还会要求安装与其相关的语言组。例如，要使用德语 UI，必须先安装西欧和美国语言组。

既可在安装 Windows 2000 时安装和卸载 Windows 2000 语言组，也可在以后通过“控制面板”的“区域选项”来完成。因为多语种版本文件的安装与删除是与语言组安装的相对独立的过程。

磁盘空间

在一台计算机上每选择多增加支持一种语言组都需要额外的磁盘空间。表 23.11 列出了每个语言组大约需要的空间。

表 23.11 语言组所需的磁盘空间的大概值

语言组	所需空间，以 MB 为单位（估计值）
阿拉伯语	1.6
亚美尼亚语	11.5
波罗的海	1
中欧	1.2
塞瑞利克语	1.2
格鲁吉亚语	5.8
希腊语	1
希伯来语	1.4
印度语	0.25
日语	58
朝鲜语	29.4
简体中文	32.5
泰语	3.9
繁体中文	13.5
土耳其语	0.9
越南语	0.5
西欧和美国	10.1

备注：很多文件（主要是字体和键盘布局）是由多个语言组共享的。因而，如果安装多个语言组，所需的总空间可能会略小于表格所列值的和。

此外，对于选择安装的每种用户界面语言，多语种版本文件的安装至少要使用 45 MB 磁盘空间。

安装

Windows 2000 多语种版本的安装包括两个步骤：

1. Windows 2000 的安装
2. 多语种版本文件的安装

如果在安装相应的多语种版本文件之前，安装 Windows 2000 期间安装必需的语言组，那么在安装多语种版本时，就可以不必在安装多语种时换光盘。

安装多语种版本时决定 UI 语言的默认值（指默认情况下，计算机中创建的所有新用户帐户所应用的语言）。可用 Muisetup.exe 文件更改默认的 UI 语言或添加或删除 UI 语言。

备注：用 Muisetup.exe 文件添加和删除语言将只影响多语种版本文件。要添加或删除与语言组相关的文件，可用控制面板的“区域选项”。

有关自动执行 Windows 2000 安装的详细信息，参见本书中的“服务器自动安装与升级”和“使用 Systems Management Server 部署 Windows 2000”。

使用组策略管理 UI 语言

如果用多语种版本减少单位中客户配置的数量，将会大大简化管理客户工作。但是，若所有用户均可更改其计算机的 UI 语言，则会为环境增加不必要的复杂性。因此，您可能想限制某些用户更改其 UI 语言的权限。可通过组策略管理单元的“用户配置”节点，应用组策略来达到此目的。

但请注意：如果用本地组策略把多语言策略应用于本地计算机，那么本地组策略对象将会影响该计算机的所有用户，原因是无法为个别用户筛选本地组策略对象。

有关 Windows 2000 多语种版本的详细信息，参见 Web 资源页中 Windows 2000 Professional 多语种支持的链接，网址是：
http://windows.microsoft.com/windows2000/reskit/webresources。

使系统更易使用

有特殊要求的用户往往比其他用户更易受到其计算机界面的影响。您的规划目标之一应该是为每个人，包括有视觉、听觉、行动或认知障碍的人，提供使用计算机软件的平等权限。

不应将全部有认知障碍的人都划分在相同的类别中；他们的要求也是多种多样，这与任何其他类型的用户一样，甚至更加复杂。应考虑下列人士所面临用户界面多种问题：

- 视觉障碍。包括失明、视力低下和色盲。
- 听觉障碍。包括失聪或部分听力丧失。
- 行动障碍。包括脑中风、发抖、癫痫症发作、手指或肢体残缺及瘫痪。甚至有腕管综合症或其他重复性拉伤的人，均可视为有行动障碍的人士。
- 认知障碍。包括学习障碍，如诵读困难及记忆力丧失；特瓦综合症和语言障碍，如文盲和语言不熟。

配置 Windows 2000 功能使其具有辅助功能

因为每个人的具体要求不同，所以不同用户会发现 Windows 2000 不同方面所具有的挑战性。表 23.12 列出了在配置 Windows 2000 和 Windows 2000 中特定的新的和升级的辅助功能时，应考虑的几个一般性注意事项。

表 23.12 在 Windows 2000 中配置辅助功能

功能	定义
Microsoft 工具管理器	工具管理器使计算机中的辅助功能应用程序更易于访问，并简化配置这些选项的过程。
Microsoft 辅助功能向导	辅助功能向导可根据障碍类型（而不根据数值变化）指定选项，从而简化设置常用辅助功能的工作。
Microsoft 屏幕键盘	屏幕键盘使有行动障碍的用户能够利用它进行有限的访问。
Microsoft 讲述人（带内置的文本到语音功能）	讲述人是一种合成的、功能有限的文本到语音工具，可供有中等视力缺陷的用户使用。讲述人可大声朗读显示在屏幕上的内容。

Microsoft 放大镜	放大镜是一个基本的屏幕放大器，可在独立的窗口显示屏幕的一部分。
高可见度的鼠标指针	全新的大型、超大型、白色或黑色指针。此外，反转的指针会变成与背景反差大的颜色。
高对比度配色方案	扩展的配色方案库能够帮助视力较差的用户，这些用户要求前景色与背景之间的对比度很高。
快速启动栏	在任务栏的快速启动栏中，辅助功能状态图标向用户显示：是否通常使用的键盘筛选器处于活动状态。
同步可访问媒体互换 (SAMI)	启用多媒体产品的字幕显示。

启用第三方设备

虽然 Windows 2000 中的辅助功能工具为有特殊需求的用户提供了一些功能，但是大部分残疾用户在日常使用中，还需要其他工具。Windows 2000 中的 Microsoft 活动辅助功能 (MSAA) 也是一项新的功能，它是一种可使使用辅助功能的人也能使用 UI 元素（如工具栏、菜单、文本和图形）的 API。

小型或大型键盘、目控指示设备，以及通过呼吸控制的吸吹系统都是附加软件的举例。还有一类称为增强式通信设备，它们最初是专为语言表达有障碍的人而设计，用于控制语音合成器。

用户可能会注意到这些产品，并会告诉您，他们希望在其计算机中启用哪些功能。有关需要辅助功能人士所用硬件和软件的详细信息，参见 Web 资源页的 Microsoft Accessibility 链接，网址是： http://windows.microsoft.com/windows2000/reskit/webresources。

使用组策略精细调整辅助功能配置

可通过组策略访问的大量配置选项将会对那些需要辅助功能的用户有所帮助。可与某位具有丰富辅助功能问题知识的人士（人力资源部通常会有这方面的专业人士）共同审阅您的用户界面配置选项，以便为需要使用辅助功能的人士配置计算机。

同时，当您开始规划高级更改与配置管理时（参见本书的“ 应用更改与配置管理 ”一章），如果能使需要辅助功能的用户使用这些功能，使其发现不再局限于一台满足其要求的计算机上工作，这样的规划应是很有意义的工作。

客户标准规划任务列表

表 23.13 中总结了准备 Windows 2000 的客户管理与配置标准时需要执行的任务。

表 23.13 客户配置规划任务列表

任务	本章中的位置
定义客户管理策略。	定义管理模型和标准
根据职能定义客户应用要求。	定义软件标准
根据职能定义客户配置限制	配置硬件
配置获准的客户硬件（便携式和台式计算机），以运行 Windows 2000。	配置硬件
配置基本的 Windows 2000 用户界面选项。	使客户系统可管理
登录与注销选项	使用组策略进行配置控制
“ 开始 ”菜单选项	使用组策略进行配置控制
桌面选项	使用组策略进行配置控制
多语种选项	添加多语种选项
辅助功能选项	使系统更易使用
根据客户要求和管理指南配置应用程序。	定义应用程序要求

必要的应用程序	定义应用程序要求
可选的应用程序	定义应用程序要求

第 24 章 - 应用更改与配置管理

客户计算机的配置，以及桌面型和膝上型计算机的使用方式，已经变得越来越复杂。信息技术(IT)需要提供给用户的解决方案和服务也变得越来越复杂。Microsoft® Windows® 2000 提供了一些高级的更改与配置管理功能，即使当用户使用其他计算机时，他们的用户设置、文档和软件还是可用的。此外，这些启用了 Active Directory™ 的功能使您可以在用户计算机硬盘或其他组件发生故障时为它们提供一个几乎完全相同的替代物。

本章将概述在 Windows 2000 中实施通常称作 IntelliMirror™ 的高级客户管理功能所需的规划步骤。您还会学习如何将远程操作系统(OS)安装并入客户支持规划。在阅读本章之前，您要理解并完成在“定义客户管理和配置标准”和“设计 Active Directory 结构”章节中定义的规划步骤。

本章内容

评估更改与配置管理
启用远程 OS 安装
使用组策略改善软件管理
维护网络中的用户数据和设置
为您的单位选定更改与配置管理选项
更改与配置管理规划任务列表

本章目标

本章将帮助您制定以下规划文档：

- IntelliMirror 实施规划
- 远程 OS 安装实施规划

资源工具包中的相关信息

- 有关基本客户配置选项和使用组策略管理 Windows 2000 客户的详细信息，请参见本书的“定义客户管理和配置标准”。
- 有关使用 Systems Management Server 的详细信息，请参见本书中的“使用 Systems Management Server 部署 Windows 2000”。
- 有关测试和先导测试 Windows 2000 技术的详细信息，请参见本书中的“建立 Windows 2000 测试实验室”和“实施 Windows 2000 先导测试”。

评估更改与配置管理

当用户的计算机出现问题时——例如软件不能运行、文件丢失或者是硬件发生故障——IT 支持人员通常需要本人去查看计算机以分析并解决问题。数百或数千以上的客户计算机，包括数量增加的频繁从网络上断开的计算机，以及多个用户使用的计算机，都属于网络管理员面临的最昂贵的支持问题。

Windows 2000 提供了许多更改与配置管理技术，这些可以帮助 IT 部门减少工作量以及管理和支持客户计算机的相关成本。将“定义客户管理与配置标准”章节中创建的管理和配置标准作为基础，通过启用以下支持 Active Directory 的用户服务，可以减少计算机替换过程中的工作量和时间。

远程 OS 安装可以使系统管理员简化并减少筹备和配置新的或替换的客户计算机的成本。此外，远程 OS 安

装利用预先配置的一个操作系统和基本应用程序，改进了 IT 迅速恢复故障系统的能力。

软件安装与维护允许系统管理员指定一套用户或用户组始终可以使用的应用程序。如果某个必要的应用程序在需要时还未在计算机上安装，这个应用程序就会被自动安装。同样地，如果一个应用程序需要修复（例如由于某个文件被损坏或意外删除）、更新或删除，这样的任务都可以自动执行。

用户设置管理 “ 定义客户管理与配置标准 ” 章节中说明了如何自定义和控制用户界面。在本章节中，您将学习如何实施漫游用户配置文件。使用漫游用户配置文件，用户配置文件设置和应用于用户的组策略设置，都复制到用户可能登录的网上任意一台计算机上。

用户数据管理
允许用户漫游到公司网上任一基于 Windows 2000 Professional 的计算机并能访问他们的数据。此外，如果用户将基于网络的资源脱机，这些资源将在用户再次连接到网络上时重新同步。

后面的三种能力被归组在 IntelliMirror 名下。IntelliMirror 和远程 OS 安装一起构成了 Windows 2000 更改与配置管理，大大减少了替换计算机所需的工作量和时间。图 24.1 举例说明了这些功能的规划过程。

图 24.1 IntelliMirror 和 远程 OS 安装的规划步骤

用来启用更改与配置管理的技术

IntelliMirror 和 远程 OS 安装并非 Windows 2000 中分立的技术。这些功能利用了许多您可能已经利用的 Windows 2000 的技术。图 24.1 举例说明了实施 IntelliMirror 和远程 OS 安装所需的技术。

表 24.1 启用 IntelliMirror 和远程 OS 安装使用的技术

功能	使用技术
用户设置管理	Active Directory 组策略 脱机文件夹 漫游用户配置文件
用户数据管理	Active Directory 组策略 脱机文件夹

	同步管理器 磁盘配额 漫游用户配置文件
软件安装与维护	Active Directory 组策略 Windows 安装服务 添加/删除程序 分布式文件系统 (Dfs)
远程 OS 安装	Active Directory 组策略 远程安装服务（RIS） 远程安装（可能的工作站）

您可以分别实施远程 OS 安装和 IntelliMirror 用户数据管理、用户设置管理以及软件安装和维护，或任意组合其中的两个或三个。您还可以将所有四个作为一个集成的更改与配置管理解决方案实施，此方案是为在设备故障时提供快速、几乎准确、自动的计算机替换而设计。

备注 替换被描述为“几乎准确”，是由于有些用户可能在不适当的地方存储数据文件，这样文档可能无法复制到服务器上。此外，特别大的文件，例如某些邮箱或数据库文件，由于网络的带宽、服务器的磁盘空间以及同时在服务器和客户计算机上维护当前副本所需的同步时间，管理起来有相当难度。

明确更改与配置管理需求和机会

Windows 2000 更改与配置管理功能可以帮您处理很多管理问题。以下是单位使用 IntelliMirror 和远程 OS 安装的典型情况：

- 为新雇员配置计算机
- 安装和管理软件
- 备份公司数据
- 计算机故障恢复

这些问题适用于所有高级和基础类型的用户组，移动的、漫游的、远程的、基于任务的和基于知识的。这些我们都在“定义客户管理和配置标准”这一章节中讨论过。将首选的客户配置和客户管理规划作为 IntelliMirror 和远程 OS 安装实施规划的基础。IntelliMirror 和远程 OS 安装实施规划将对此进行扩展，并有助于帮助满足先前在 Windows 2000 部署规划中确定的管理方面和客户的要求。

主要背景信息

以下的背景信息对 IntelliMirror 和远程 OS 安装的规划是特别重要的：

- 您的单位会多快迁移到 Windows 2000 Professional 和 Windows 2000 ？

  只有在启用 Active Directory 的 Windows 2000 Server 的基础结构下运行 Windows 2000 Professional 的客户，才能使用 IntelliMirror 和远程 OS 安装。

  备注 Windows 2000 终端服务的客户还可以利用 IntelliMirror 和 远程 OS 安装。由于终端服务客户必须安装这些应用程序，完全的终端服务客户不能参与软件安装和维护。以管理员模式运行的终

端服务客户可以利用软件安装和维护。有关终端服务的详细信息，请参见本书的“部署终端服务”。

- 现有的客户计算机是否满足了远程 OS 安装的远程启动只读内存(ROM)和预启动运行环境(PXE)的前提条件？

  IntelliMirror 功能不要求比运行 Windows 2000 Server 和 Windows 2000 Professional 更快的处理器或更大的内存。但是，要使用远程 OS 安装的客户必须有支持的网卡或 Remote Boot ROM 版本 99b 或更高。

- 用户有什么要求？他们是否在不同位置漫游？他们是否使用多个计算机？他们是否频繁地断开与网络的连接？他们的应用程序需求是固定的还是经常变化的？

  您的目标应该是完全按照用户的要求提供这些管理功能。有关将 IntelliMirror 和远程 OS 安装与用户要求相结合的详细信息，请参见本章中的“为单位选择更改与配置管理选项”部分。

- 您单位的网络连接有多快？用户是否经常用低速的链接来连接？是否有能支持如自动软件安装和升级这样功能的网络带宽容量？

  需要在所有建议使用模式下测试和先导测试 IntelliMirror 和远程 OS 安装规划，以便决定实施更改与配置规划需要几个服务器和多大的网络容量。

- 想如何管理计算机帐户？安装 Windows 2000 Professional 的用户是否创建他们自己的计算机帐户并自定义他们自己的操作系统设置？或 IT 人员是否预先定义帐户和设置，为计算机作前期部署？

  通过组策略和安全设置的的组合，远程 OS 安装支持用户管理和 IT 人员管理的两种可选方案。

- 客户计算机的管理严密还是松散？成本最高的客户管理问题有哪些？使用更改与配置管理技术能不能使这些问题得到解决或减轻？每隔多长时间对现有应用程序进行升级或分发新的应用程序？

  如果还没有收集到这些问题的数据，请查看“定义客户管理与配置标准” 这一章。

- 单位中是否已经部署了 Active Directory 和域结构？单位中 Active Directory 和域结构背后的管理和逻辑的基本原理是什么？此外，单位中是否启用了动态主机配置协议 (DHCP) 和域名服务器 (DNS) 服务？

  有关完成这部分 IT 基础结构的详细信息，请参见“设计 Active Directory 结构”中有助您为更改与配置管理规划建立坚实基础的重要规划信息。

使用 Systems Management Server 补充 IntelliMirror

许多环境复杂的单位通过使用 Systems Management Server 2.0 提供的高级的更改与配置管理工具作为 IntelliMirror 和远程 OS 安装的补充。这些工具包括：

规划工具 Systems Management Server 使用 Windows 管理规范（WMI）和软件扫描仪检索和加载详细的硬件和软件清单（例如测试应用程序使用）到基于 Microsoft® SQL Server™ 的储备库中。这一规划工具集有助于理解环境的配置、完成审核和适应性检查、监视和限制应用程序的使用以及规划新的软件部署和升级这样的操作。

部署工具使用 Systems Management Server ，可以计划并同步化基于 Windows 的计算机的软件部署，包括 Windows 3.x、Windows NT® 3.51/4.0 和 Windows 2000。分发和清单是完全集成的，以使目标定位精确，同时可以对每个计划的部署的进展和成功与否提供详尽的状态报告。使用 Systems Management Server，可以为一台、十台或上千台的计算机在后台分发和安装软件，甚至在无用户登录时也可以。Systems Management

Server 还可以部署使用新的 Windows 安装服务技术和程序包的软件。

诊断工具 Systems Management Server 提供一系列高级远程诊断工具，使您不用到现场就可以管理桌面计算机和服务器。这包含了一些工具，如远程控制和远程重新启动、配备了分析网络状况和性能的实时和捕获后专家的网络显示器，以及显示 Windows 2000 Server 和 Microsoft® BackOffice® 关键性能信息的服务器 HealthMon 工具。

是分别使用还是一起使用 IntelliMirror 和 Systems Management Server 取决于环境的复杂程度。图 24.2 说明了可能对不同复杂程度的单位都具最好性能价格比的 Microsoft 管理解决方案。

表 24.2 推荐的更改与配置管理解决方案

	单一局域网 (LAN)/LAN 速互连的简单多 LAN	复杂多 LAN/多站点系统
仅限基于 Windows 2000 的系统	IntelliMirror 远程 OS 安装	IntelliMirror 远程 OS 安装 Systems Management Server
混合的 Windows 环境，包括基于 Windows 2000 的系统	IntelliMirror 远程 OS 安装 Systems Management Server	IntelliMirror 远程 OS 安装 Systems Management Server
Windows 3.x, Windows NT 3.51/4.0	Systems Management Server	Systems Management Server

图 24.3 说明了如何将 IntelliMirror、远程 OS 安装和 Systems Management Server 并入有效的更改与配置管理解决方案。

表 24.3 有效的更改与配置管理选项

	远程 OS 安装	IntelliMirror	Systems Management Server
安装基于 Windows 2000 的桌面映象	X	--	--
启用数据、软件和设置跟随用户	--	X	--
基于 Windows 2000 的系统的基本故障恢复	X	X	--
管理非基于 Windows 2000 的环境。	--	--	X
清单、高级部署、疑难解答和诊断工具	--	--	X
综合更改与配置管理	X	X	X

使用这些表格中的信息以及自身对单位客户管理问题的理解，来选择对单位最适合的功能。

有关联合使用 Systems Management Server 与 Windows 2000 的详细信息，请参见本书中的“使用分析网络基础结构”和“使用 Systems Management Server 部署 Windows 2000”。有关 Systems Management Server 的综合技术信息，请参见《Microsoft Systems Management Server Resource Kit》。

使用 IntelliMirror 规划增强的客户支持

本章的其他部分将指导部署 IntelliMirror 和远程 OS 实施中改进客户支持所涉及的配置和解决关键性问题的步骤。

如果客户管理标准包含用户数据的存储或网络服务器的设置，那么您可能想创建基本客户映象和网络基本结构（即服务器共享和组策略设置），以便在开始部署客户之前支持这一目标。

部署客户方法的选择包括两部分：

- 部署基本操作系统
- 部署应用程序

对于象使用 Sysprep 或 Systems Management Server 这样的备用部署方法，可以使用远程 OS 安装来部署基本应用程序和 Windows 2000 Professional。这就需要对应用程序部署策略仔细规划以决定：

- 使用远程 OS 安装的操作系统应部署哪些应用程序。
- 哪些应用程序在安装操作系统后使用软件安装和维护部署。
- 怎样支持最初用远程 OS 安装所安装的应用程序的重新安装和修复。

在远程 OS 安装的过程中安装一套核心应用程序能够简化配置符合单位标准的计算机的过程。但是，这并不消除在已经装有 Windows 2000 Professional 的计算机上支持安装的需要。所以，在远程 OS 安装过程中和 Windows 2000 一起安装的应用程序也应该包括在 IntelliMirror 软件安装和维护的规划内。

以下部分讲述有助于单位使用远程 OS 安装、IntelliMirror 软件安装和维护以及 IntelliMirror 用户数据和设置管理的关键规划问题。最后一部分，“放在一起”，就一些需求类型不同的单位如何实施 IntelliMirror 和远程 OS 安装提供了推荐意见。

启用远程 OS 安装

Windows 2000 远程 OS 安装为计算机在最初启动顺序过程中连接到 Windows 2000 网络服务器提供了一种方法，还使服务器能够在客户计算机上安装 Windows 2000 Professional。远程 OS 安装使管理员能够配置 Windows 2000 和任何想和操作系统一起安装的应用程序，一旦为一组用户安装了操作系统，即可将同一配置用于单个客户机上操作系统的安装。对用户来说，结果是计算机的安装和配置既简化又及时。而且当硬件故障发生时，可以更快地恢复生产力。

表 24.4 列出了使用远程 OS 安装需要掌握的 Windows 2000 技术。

表 24.4 使用远程 OS 安装需要的 Windows 2000 技术

技术	目的
动态主机配置协议(DHCP)	联系运行 RIS 的服务器前为启用远程启动的客户计算机指派 IP 地址。
域名服务器(DNS)	通过 TCP/IP 地址解析计算机名。
组策略	定义合格的（或不合格的）用户和计算机以接收给定的桌面配置。
Active Directory 服务	定位客户计算机和 RIS 服务器，并存储定义什么资源用户或计算机能或不能访问的组策略对象。
远程安装服务(RIS)	管理和分发 Windows 2000 Professional 映象文件到启用远程启动的客户。

如果还没有安装和配置 DNS、DHCP和 Active Directory，请参见本书“定义 Active Directory 结构”章节完成这些规划步骤，然后继续本章。还应理解“定义客户管理和配置标准”章节中概述的组策略规划步骤。本章节剩余的部分将集中讲解 RIS 不同组件的相关规划，以及如何将其配置为一个有效的部署。

定义用户要求

所有用户，无论其技能层次或计算要求如何，当系统出现故障或得到一台新的计算机时都需要一个快速、有效的方法来安装新的操作系统和核心应用程序。为了减少为用户预配置新系统的相关时间和成本，需要回答以下的问题：

为这些用户安装操作系统的最佳方法是什么？在一些小型分支机构的办事处或家庭办公室，没有足够的用户以保证 RIS 服务器安装需求，或者用户需要旅行，没有和网络服务器的高带宽连接，使用 CD-ROM 或其他方法安装操作系统可能是最佳选择。对于有高带宽网络连接，但计算机没有远程启动兼容的网卡或远程启动 ROM 的用户来说，基于网络的映象复制或手动安装方法是下一个最佳选择（有关详细的信息，请参见本书中的“自动执行客户安装与升级”）。对于所有其他需要一个新的、已知的 Windows 2000 Professional 配置的情况，请使用远程 OS 安装。

用户应有多大自由选择可选的操作系统组件或备选操作系统映象？以下部分描述了一些可以用于配置远程 OS 安装映象的可选设置。在大多数情况下，您会希望对知识不很丰富或不太以任务为主导的用户少给或不给操作系统安装的可选项。Windows 2000 Professional 安装过程中，高级的、有丰富知识的用户可能要求额外的选项。

使用远程 OS 安装

从最终用户的角度来看，远程 OS 安装的过程比较直接。这是由于 IT 部门有下列现成的配置，工作也就基本上完成了：

- 为每组用户确定如何配置操作系统。
- 将用户限定于您认为合适的尽可能少的几种操作系统配置。

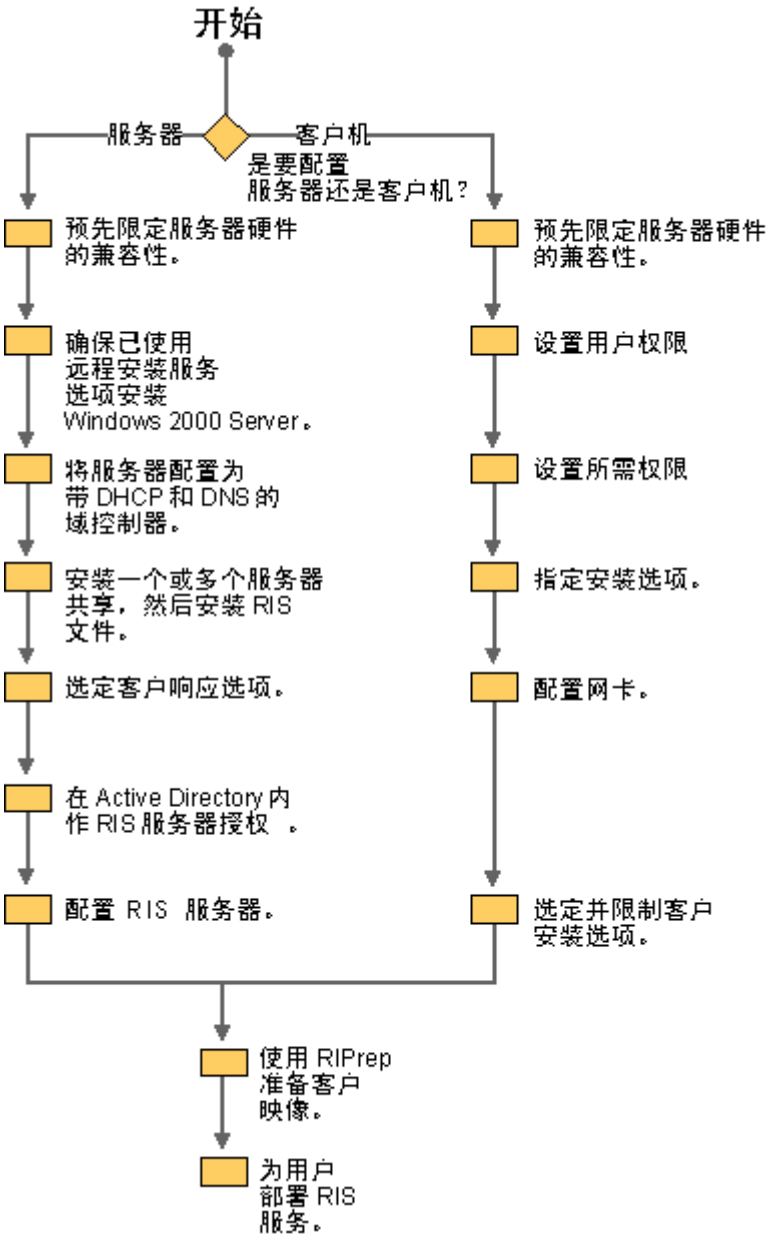
- 通过预先确定最终用户可以修改的安装选项（如果存在）以指导用户成功安装操作系统。

远程 OS 安装中涉及 RIS 的五个主要组件：

- **远程安装服务的安装程序(RISetup.exe)**用于安装 RIS 服务器。
- **远程安装服务管理员。**用于配置与 RIS 服务相关的组策略设置。
- **远程安装准备向导(RIPrep.exe)。**用于创建操作系统映象并安装于 RIS 服务器。如果想在操作系统上安装应用程序，也可以使用 RIPrep 创建应用程序映象。
- **远程安装启动软盘(RBFG.exe)。**用于创建在特定客户计算机上安装基于 RIS 的操作系统所需的启动软盘。
- **客户安装向导(OSChooser.exe)。**用于在客户计算机上选择用户需要安装的 RIS 映象

所有符合 PC98 版本 0.6 或更高版本的设计规范都包含一个用于远程 OS 安装的预启动运行环境（PXE）远程启动 ROM。现有未包含 PXE ROM 的客户计算机可以使用远程安装启动软盘来创建可以初始化 RIS 过程的软盘。RIS 远程启动软盘可以和很多有支持的基于外设部件接口（PCI）的网卡一起使用。有关详细信息，请参见 Windows 2000 操作系统 CD 中的 Windows 2000 硬件兼容列表 (HCL) 和 Web 资源页的 Microsoft Windows Hardware Compatibility List 链接，地址是：
http://windows.microsoft.com/windows2000/reskit/webresources。

图 24.2 说明了配置远程 OS 安装的主要步骤。以下部分讨论使用 RISetup.exe、远程安装服务管理员管理单元以及 RIPrep.exe 时的主要部署规划问题。


开始
服务器
客户机
是要配置
服务器还是客户机？
预先限定服务器硬件
的兼容性。
确保已使用
远程安装服务
选项安装
Windows 2000 Server。
将服务器配置为
带 DHCP 和 DNS 的
域控制器。
安装一个或多个服务器
共享，然后安装 RIS
文件。
选定客户响应选项。
在 Active Directory 内
作 RIS 服务器授权 。
配置 RIS 服务器。
预先限定服务器硬件
的兼容性。
设置用户权限
设置所需权限
指定安装选项。
配置网卡。
选定并限制客户
安装选项。
使用 RIPrep
准备客户
映像。
为用户
部署 RIS
服务。

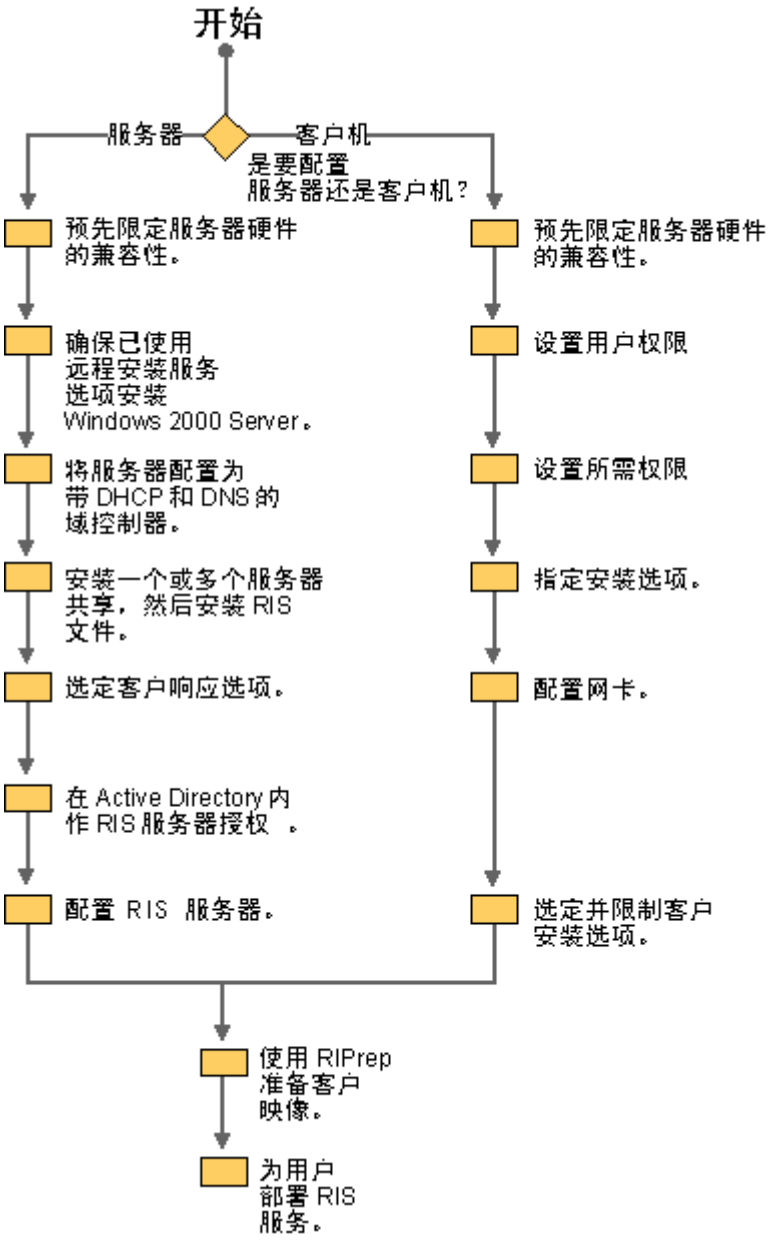


图 24.2 RIS 服务的规划步骤

配置远程安装服务

远程安装服务(RIS)是安装 Windows 2000 Server 时的可选安装组件。尽管这一安装程序大部分是自动的，当 RIS 已安装但还未向用户提供服务前，还是可以配置一些基本的和高级的设置。

默认情况下，RIS 不是在安装后立即进行配置以为客户计算机提供服务。如果需要的话，可以接受默认的 RIS 配置设置，并基于这些选项开始为用户提供安装映象。但是，多数单位会自定义 RIS 以便更好地迎合 IT 和业务的需要。

为了同时给 RIS 服务器和客户计算机配置 RIS 设置，需要使用 Active Directory 用户和 Microsoft 管理控制台（MMC）计算机管理单元。服务器配置选项确定特定 RIS 服务器怎样响应客户计算机的服务请求。客户选项帮助您定义 RIS 映象是如何安装在客户计算机上的。

可以用 Active Directory 用户和计算机管理单元设置的主要的配置选项包括：

定义自动的客户计算机命名格式 允许确定计算机名称（自动生成）是否应按用户名、用户的名加姓或是单位自定义的命名格式。默认是用户名。

为创建所有机器帐户对象定义默认的 Active Directory 位置 可以选择默认的 Active Directory 容器，或部门(OU)，或专为 RIS 客户创建一个新的 Active Directory OU。默认设置是“计算机容器”。

服务前在 Active Directory 内进行客户计算机前期部署 可以用这个选项定义在 Active Directory 内哪些客户计算机帐户可以使用远程 OS 安装。要使用此选项，需要指定客户计算机名称、默认的 Active Directory 的位置、客户全球唯一标识符(GUID)，以及为负载平衡的可选项，即哪个 RIS 服务器支持指定客户。默认设置为“没有前期部署客户”。

提供第三方 ISV 维护和疑难解答工具 使管理员和许可的终端用户能够访问从独立软件提供商(ISV)处得到安装前的维护和疑难解答工具。举例来说，这样的工具可以升级基本输入输出系统(BIOS)、检查病毒、执行计算机诊断或在安装操作系统前列出系统清单。默认值是“没有安装工具”。

在 CD 或 RIPrep 格式中添加更多的操作系统映象 可以利用这个选项为企业现有 RIS 服务器添加新的操作系统版本或 RIPrep 映象，或将多种无人参与安装模板与当前操作系统相关联。例如，可以使用此选项设置多个RIPrep 映象，而后每个映象只有单位中适合的用户才能使用。默认设置为“基于 CD 的 Windows 2000 映像”。

从 Windows 2000 Professional 工作站远程配置 RIS 服务器 启用这个选项，可以远程管理域或企业中的任何 RIS 服务器上的许多 RIS 选项。默认设置为 N/A，是指运行 Windows 2000 Professional 的计算机也能执行此处描述的绝大部分配置选项，并已经启用执行管理任务。

支持多供应商安装服务器的同时存在 这个选项支持单位使用 Windows 2000 以外的远程安装和启动服务器在同一物理网络上操作。此选项通常与前面描述过的前期部署选项一同使用，所以 RIS 不影响已有的使用同一远程启动协议的远程启动服务器。默认设置为“禁用”。

还有三个配置选项可以在 RIS 服务器属性页以外定义。这些选项是由使用组策略设置，以及对希望限制用户使用的操作系统映象设置特定安全描述符、或访问控制列表(ACL)确定：

定义可用的客户安装选项 此选项使用组策略限制用户组的安装选项。例如，您可能希望一些用户访问维护和疑难解答工具菜单或自定义安装选项。默认设置是所有用户可以使用自动安装。无其他可用安装选项。

定义可用的操作系统安装选项 此选项使用安全描述符指定必须可以访问 RIS 服务器上的操作系统映象的用户。可以使用此功能指导用户进行适合自己工作的无人参与操作系统安装。所有映象都默认“对所有用户可用”。

防止任意外来服务器的 RIS 服务器授权 此选项防止未经授权的 RIS 服务器在单位网上服务客户。必须对可以为启用远程启动的客户提供安装的 RIS 服务器进行授权。无更改选项。

准备客户操作系统映象

RIS 支持两种类型的操作系统映象，即基于 CD 的映象和 RIPrep 映象。在最简单的情况下，可以为用户提供直接的基于 CD 的操作系统安装，即以无人参与方式安装 Windows 2000 Professional。

如果想要配置 Windows 2000 Professional 的自定义安装，而不为每个类型的客户计算机和计算机上安装的每个硬件单独创建映象，RIS 通过利用 Windows 2000 中改进了的即插即用支持在安装时检测源计算机和目标计算机之间的差别来提供这种能力。

备注 如果客户计算机硬件抽象层（HAL）驱动程序不一样，不为每种类型的客户计算机和每个硬件创建单独

映像的情况下，您将不能配置 Windows 2000 Professional 自定义安装。但是，大多数工作站级别和桌面型计算机不象服务器级的计算机那样要求特有的 HAL 驱动程序。特有的 HAL 驱动程序通常区分支持和不支持高级配置电源接口(ACPI)的客户计算机。

RIPrep 可用于准备现有 Windows 2000 Professional 映象，包含所有本地安装的应用程序或配置设置，并将该映象复制到网络上的 RIS 服务器。通过在 RIS 映象中包含一套基本的应用程序，可以大大地减少设置客户计算机的工作量。有关用 RIS 和 IntelliMirror部署的打包应用程序信息，请参见本章稍后的“使用组策略改善软件管理”。

客户安装选项

要运行 RIPrep，需要回答几个基本的问题，例如将要用来存储映象的服务器的位置。回答完这些问题之后，RIPrep 向导通过删除计算机特有的东西，例如计算机特有的安全标识符(SID)，将映象配置到一般状态，然后将其复制到 RIS 服务器。

当设置 RIS 时，可以使用组策略配置以下客户安装选项：

自动安装 所有用户对自动安装选项有默认访问权限。如果许可访问单一操作系统映象，操作系统安装在用户登录时即开始，用户不需要回答任何问题。如果决定提供用户多种操作系统安装类型，将选项限制在三到五个，最大程度地避免混乱，以确保用户选择最适合单位需求的操作系统。

自定义安装 自定义安装选项使您或帮助中心职员能够为单位中的其他人安装计算机。这是通过允许覆盖管理自动计算机命名的规则和创建计算机帐户的位置而实现的。这是因为基于应用于管理员或帮助中心人员的组策略设置命名计算机或定位计算机帐户可能是不合适的。可以将此选项用于预安装客户计算机，或当 IT 或帮助中心职员必须本人访问终端用户以便重新安装计算机的情况。

重新启动前面的安装 使用此选项，可以避免要求用户重复回答有关已安装的操作系统的任何问题。例如，如果一个用户已经被提问过单位名称、部门名称、视频分辨率，“重新启动”选项，确保用户遇到安装故障后重新启动时不会被重复提问。此选项不在故障发生时重新启动安装程序。也不会试图解决前面的安装尝试中出现的问题。

维护和疑难解答选项 此选项提供对如 BIOS 升级和病毒扫描程序这样的第三方硬件和软件工具的访问。如果提供安装工具的访问权，只能允许对不会损坏计算机或导致其他问题的工具的访问权。

使用组策略改善软件管理

典型的大单位支持成百上千的程序。如果将不同版本、补丁、修正以及模板在清单中列作单独的程序，这个数字会显著地增加。

由于没有管理软件组的有效手段，很多单位都不能及时升级其应用程序软件。当他们确实决定放弃过时的软件或实施新的应用程序时，完全的改变会非常不利。

可以在以下方面通过使用 Windows 2000 简化软件管理程序：

- **准备。**想管理什么软件？想如何格式化软件进行分发和安装？
- **分发。**想从何处管理软件？
- **目标定位。**想让谁接收软件？
- **安装。**如何将软件安装在计算机上？

图 24.3 说明了每个阶段所涉及的主要规划问题。

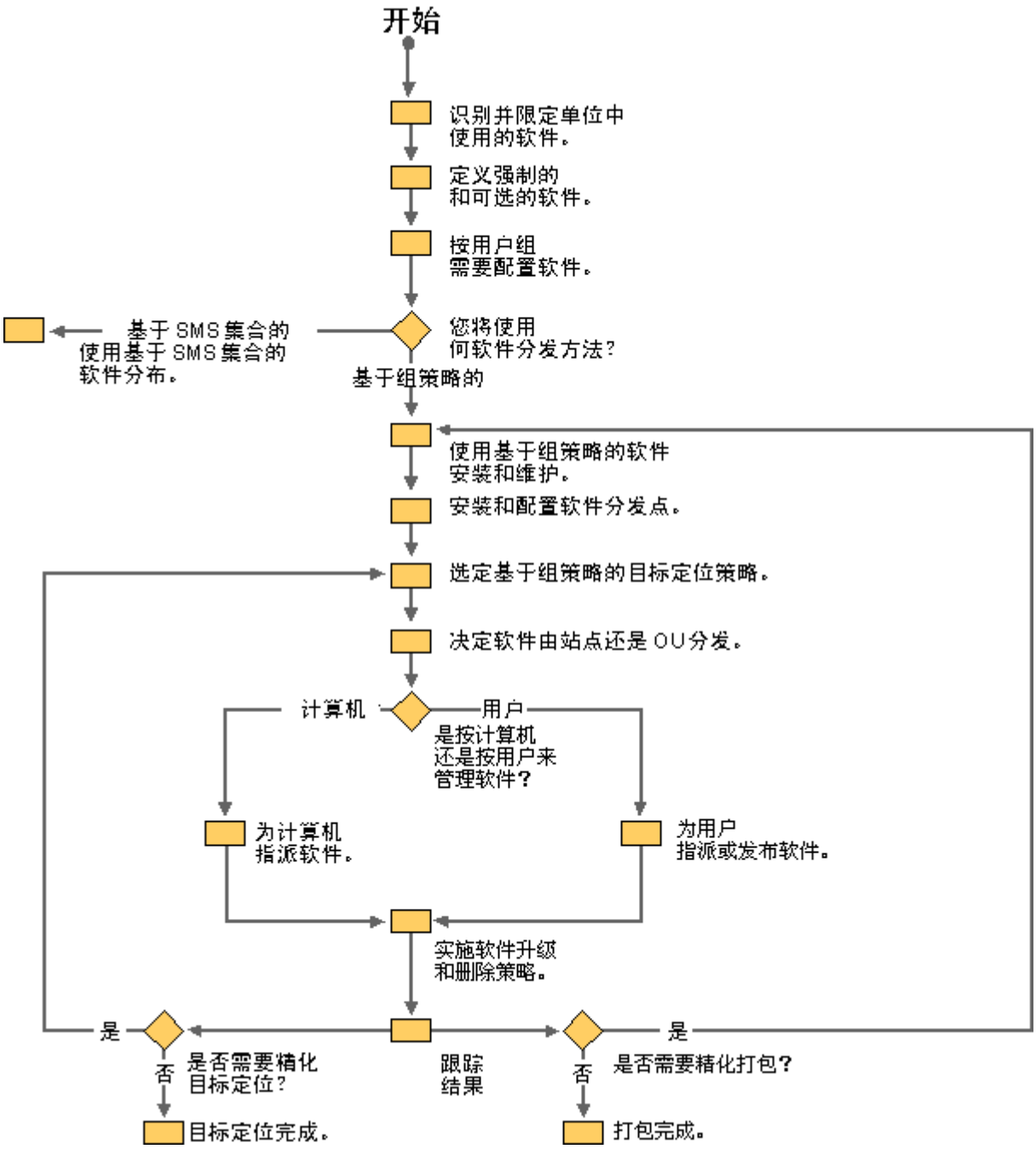


图 24.3 部署 IntelliMirror 软件时需要讨论的关键规划问题

即便是与 Windows 2000 Professional 一起安装的应用程序，也需要执行这些规划步骤。还需要在部署、升级和维护现有计算机上的应用程序时继续使用这些步骤。

为分发准备软件

在“测试应用程序与 Windows 2000 的兼容性”和“定义客户管理和配置标准”章节中，您已经评估了单位

中应用程序与 Windows 2000 的兼容性，并将其划分为可选的和强制的：

- 单位作为一个整体。
- 单位中的用户组。

在可以使用 IntelliMirror 分发软件应用程序前，需要确定已对其与 Windows 2000 一起部署进行了适当的配置。

利用了 Windows 安装服务的应用程序将能最有效地使用 Windows 2000 应用程序支持功能。Windows 安装服务是一个新的安装服务，由以下内容组成：

常驻操作系统的安装服务 在过去，每个操作系统都提供自己的可执行安装文件或脚本。因此，每个应用程序必须确保使用了正确的安装规则（例如文件版本规则）。此外，可供开发人员在编写安装例程时参考的实用指导很少。结果，指定应用程序的安装或删除通常会破坏计算机上现有的应用程序。Windows 安装服务确保操作系统实施了关键的安装程序规则。要遵循这些规则，应用程序只需以标准 Windows 安装服务格式描述自己。

组件管理的标准格式 Windows 安装服务把所有应用程序看作三个逻辑组块：组件、功能及产品。组件即是文件、注册表项以及其他已安装或未安装的资源的集合。当选择某组件进行安装或删除时，其中的资源也被安装或删除。功能即是用户可以选择安装的应用程序块。他们通常代表了应用程序本身的功能性特征。当用户在安装程序中选择“自定义安装”时，可以选择安装的应用程序块与功能大致对应。Windows 安装服务产品代表了一个象 Microsoft® Office 那样的单一产品。产品由一个或多个 Windows 安装服务功能组成。每个产品对 Windows 安装服务都是以一个 Windows 安装服务包(.msi)文件的形式进行描述。

应用程序和工具的管理 API Windows 安装服务应用程序编程接口（API）使工具和应用程序列举安装在计算机上的产品、功能、以及组件，并安装及配置 Windows 安装服务产品和功能，以及指定安装在计算机上特定的 Windows 安装服务组件的路径。编写时利用 Windows 安装服务的应用程序可以得到漫游用户支持、“请求”安装以及运行时的资源弹性。

利用 Windows 安装服务技术的原编应用程序可以支持：

- **适时功能安装。**仅允许分发应用程序的部分可选功能。然后，当用户试图使用未安装的选项（例如语法检查器或插图库），选项会在初次请求时安装。这样能节省很少使用的应用程序功能所占用的硬盘空间，同时使其对偶尔需要使用它们的用户可用。
- **功能修护。**如果关键的应用程序文件被损坏或被无意删除，Windows 安装服务将识别所需的文件并自动重新安装。
- **用提高的特权安装。**用户并不需要是本地计算机管理员才能用 IntelliMirror 软件安装和维护来安装软件。他们只需要是“user”或“power user”。

备注 许多软件供应商和内部开发小组都在利用 Windows 安装服务的功能进行应用程序升级。有关 Windows 2000 应用程序规范的详细信息，请参见此 Web 资源页的 MSDN 链接，地址在：

当不能自己编写程序时

并非所有时候都能够原编应用程序。特别是您可能有旧的应用程序，却没有原编 Windows Installer 程序包的资源。但仍可以通过重新打包这些应用程序将其用于 Windows 2000，从 Windows 安装服务功能获益。

可以用 Windows 2000 Server 带的 WinInstall LE 这样的重新打包工具来为文件进行重新打包。

原始应用程序与自定义应用程序映象之间的更改被转换到 Windows 安装服务程序包中。

重新打包的文件使您可以受益于 Windows 安装服务的功能，即，可以对其进行公布和修改，还可以以提高的特权安装。（公布以及其他分发选项将在本章稍后的“ 软件管理选项 ”部分讨论。）但是，重新打包的应用程序不能受益于 Windows 安装服务结构，即，重新打包的应用程序会象只有一个（大的）功能那样安装。

管理旧应用程序

还可以使其他应用程序对使用其现有安装程序的用户可用。为此需要使用一个文本编辑器，例如记事本，来创建一个 ZAP(.zap)文件。类似 INI 文件的 ZAP 文件放在与对应原始安装程序相同的文件夹中的软件分发点上。由于是在发行现有安装，用户的经历不会优于现有安装。如果现有安装不支持软件的干净和完全的删除，则发行现有安装不会改进软件删除的经历。通过管理使用 ZAP 文件格式的软件文件，应用程序会在控制面板的“ 添加/删除程序 ”中出现，用户就可以从此位置安装这个应用程序。

备注 用户仍需要与旧应用程序的要求相同的管理员特权以完成此类型的安装。

有关管理旧应用程序的详细信息，请参见《Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide》中的“ 软件管理 ”。

使用转换

过去，想自定义安装行为的管理员必须通过直接修改安装脚本重新打包应用程序以达到希望的结果。如果许多不同的安装脚本需要类似的更改，管理员就需要为每个脚本重复这些工作。

使用 Windows 2000，不再需要自定义 Windows 安装服务程序包来自定义单位的安装。取而代之的，可以创建转换并使用此转换自定义对象包。Windows 安装服务转换在部署时修改 Windows 安装服务程序包文件，因此动态地影响安装行为。

可以转换或自定义 Windows 安装服务程序包来处理多种自定义。例如，转换可以被用于将选择的功能安装在一个预先定义好的位置，这样用户不用决定安装什么功能，以及在哪里安装。还可以使用转换来修改指定组件的路径，只要组件是存在于修改的程序包中。

尽管现有的安装服务器通常对指定的功能通过用户“ 已安装 ”和“ 未安装 ”两种选择，Windows 安装服务功能仍然可以设定为以下四种状态之一：

- **安装在本地硬盘上。**文件复制到本地计算机的硬盘上。
- **安装成从资源运行。**文件保留在资源上（通常为网络共享或 CD）。应用程序从资源访问文件。
- **已公布的文件。**文件保留在资源上，但可以在第一次使用时安装在硬盘上。
- **未安装。**没有文件被复制。

转换应存储在与其自定义的 Windows 安装服务程序包相同的网络共享上。转换在部署时应用，并且不能应用于已安装的应用程序。

分发软件

当软件已经准备好（即，软件已经是适当的程序包格式，而且任何自定义或转换已经创建），可以移动实际的软件文件（包括程序包和任何转换）至遍布单位的一系列网络共享。通常，这些软件的分发点遍及整个单位，所以人们总是可以从提供可靠、高速的连接的分发点得到软件。

Windows 2000 软件安装和维护不直接讨论分发阶段。部署小组负责测试软件分发规划，并确保网络带宽、安装服务器的放置和数量足够满足单位的预期需求。

但是还可以使用其他 Windows 2000 服务，例如 Microsoft 分布式文件系统(Dfs)，来管理分发阶段。有关规划和部署 Dfs 卷的详细信息，请参见本书中的“确定 Windows 2000 存储管理策略”。

确定软件目标

IT 管理员需要按照用户执行工作的方式为整个单位安装应用程序。由于用户对软件的需要和本身的计算机知识的层次不同，IT 通常要分发这样的组合：

- 通用应用程序，如所有用户都必须使用的电子邮件和字处理软件。
- 执行特定任务或属于特定部门或分支的用户所需要的任务相关的应用程序。
- 用户根据需要可选择安装的应用程序。

在部署规划的这个时候，您应该能够确定：

- 哪些用户应该收到什么应用程序。
- 在站点层次、域层次以及部门（OU）层次需要设定哪些应用程序管理的组策略设置。

备注 尽量避免在可能应用于同一个人的不同组策略对象中管理同样的应用程序，例如 Microsoft Word。

要使用组策略定义目标，需要使用组策略和软件安装管理单元。使用组策略管理单元，可以创建一个新的或编辑现有的组策略对象，以及指派或发行软件到用户或计算机。

软件安装管理单元生成应用程序公告脚本，并将其存储在 Active Directory 和组策略对象的适当位置。

有关与站点和 Ou 共同使用组策略的详细信息，请参见本书的“设计 Active Directory 结构”。有关使用组策略实施客户机标准的详细信息，请参见本书的“定义客户管理和配置标准”。

软件管理选项

基于组策略的软件部署是为了简化在整个生命周期管理软件的过程而设计的。可以使用软件安装和维护来指派或发行应用程序、升级部署的应用程序、安装服务程序包以及删除不再需要的应用程序。所有这些任务都可以在无用户干涉的情况下进行。Windows 2000 组策略允许基于三种标准分发应用程序：

为用户指派应用程序 当为用户指派应用程序时，不管用户登录到哪台计算机上，应用程序总会出现在用户的“开始”菜单中。当用户启动未在本地计算机上安装的指派应用程序时，应用程序会先安装，然后运行。如果用户删除指派的应用程序，这个应用程序的快捷方式会重新出现在“开始”菜单中。总体而言，应该给用户指派所有强制的（通用的和特定作业的）应用程序。

为计算机指派应用程序 与指派给用户的应用程序不同，指派给计算机的应用程序在计算机下一次启动时安装。如果多个用户使用一台计算机，并且他们都使用同样的应用程序，那么那个应用程序就是指派给计算机侯选应用程序。许可站点病毒扫描软件为可能指派到计算机的软件的例子。此外，为仅当用户使用特定计算机时才需要应用程序时给计算机指派应用程序，例如图书馆里的计算机。

发行应用程序 当发行应用程序时，它们不在“开始”菜单里出现。它们必须使用控制面板中的“添加/删除程序”手动安装。“添加/删除程序”检索 Active Directory 中已发行的应用程序列表。用户可以从计算机上删除已发行应用程序，且这些应用程序不会在他们的计算机上再次被公告。当站点、域或 OU 上的所有用户都不需要某应用程序，但它可能对有些用户有用时，发行该应用程序。不能把旧的应用程序指派给一个用户或计算机。它们只能被发行。

备注 如果希望不管用户怎样做，应用程序总是被安装，或能够被安装，就要为用户或计算机指派软件。发

行对应用程序与用户或计算机之间的连接不如指派应用程序那么紧密。

用户双击其文件扩展名已和这个应用程序建立连接的文档时，已指派或已发行的应用程序也可以被安装。图 24.5 提供了为用户或计算机指派应用程序，以及发行应用程序之间的差异的其它信息。

图 24.5 指派的和发行的应用程序之间的行为差异

	已指派给用户	已指派给计算机	已发行
部署后，软件何时可用？	下次登录后。	在下一次计算机启动或重启时。	下次登录后。
用户通常从何处安装软件？	“开始”菜单或桌面快捷方式。	软件已安装。	控制面板中的“添加/删除程序”。
如果软件还未安装，并且用户打开了与软件关联的文件，软件是否开始安装？	是。	软件已安装。	是。
用户是否可以使用控制面板中的“添加/删除程序”删除软件？	是，且软件可立即再次用于安装。	否。只有本地的管理员才能删除软件。	是，并且可以从控制面板的“添加/删除程序”中选择再次安装。
支持哪些安装文件？	Windows 安装服务程序包。	Windows 安装服务程序包。	Windows 安装服务程序包及旧的应用程序。

指派或发行软件所涉及的实际步骤是类似的。管理员都是从软件安装管理单元完成这两项工作。具体任务在管理单元的帮助文件中作了描述。

应用程序通常是在管理较严的单位中被指派，特别是支持成本有问题，且多用户共享计算机的单位。在管理不是很严的单位里，应用程序通常是发行多于指派。

支持漫游用户

在许多单位里，某些人员因工作原因从一个位置移动到另一个位置，例如，接待员经常互相替班。尽管这些雇员登录到不同的计算机，他们总是有高速或 LAN 连接。

Windows 2000 软件安装和管理可以通过在用户需要时即在任何他们使用的计算机上安装他们使用的任何应用程序而改进漫游用户的 IT 支持。同样的，如果一个以前已发行的应用程序被卸载，该应用程序会在用户再次登录时删除，无论他们使用哪台计算机。

可以选择为这些用户指派软件。当他们从一台计算机移动到另一台时，会看到他们的应用程序。但是，需要将组策略设置配置为仅在用户确实想运行时才安装应用程序。

支持共享计算机

在很多单位，大家共享计算机。如果在工厂车间、培训室或实验室有计算机，可能需要支持共享的计算机。

在这些情况下，您可能更希望为计算机而不是用户指派软件。这样您就能够更为有效地管理软件，而且当用户卸载软件时，可以在计算机重启时立即重新安装软件。

考虑在这些共享计算环境中使用远程 OS 安装。然后，如果必须重建整个环境，可以采用一种有效的方式。

支持移动工作人员

更来越多的雇员，象销售人员和咨询顾问，为完成他们的工作要大量出差。尽管这些用户通常登录到同一台计算机上，他们有时候通过高速线路，有时通过低速拨号连接连接到网络上。默认情况下，软件安装和维护策略不应用于低速链接。无论操作是原始安装还是升级都是如此。有关为低速链接配置组策略的更多信息，请参见本书的“定义客户管理和配置标准”。

可能希望为这些用户发行软件并确保软件的所有自定义都在用户的本地计算机上作了安装（不同于把功能留到第一次使用时安装或从网络上运行。）

可能还希望允许移动工作人员出差时在本地媒体上保留一些软件。例如，如果一个移动工作人员经常做演示，比较值得的方法是给他一张 Microsoft Office CD 以便他随时随地都可以安装或修补重要的文件。

使用 IntelliMirror 维护软件

系统管理员需要能够在软件的整个生命周期中管理软件。IntelliMirror 软件安装和维护的设计有以下对软件生命周期的考虑：

1. 软件的生命周期开始于软件的首次部署。用户已经学会了软件并正有效地使用它。由于这是一种稳定的和已知的状态，系统管理员希望保持这种状态。
2. 但是，由于业务需要或新的、改进的软件版本的出现，就不得不考虑部署新的版本。在先导测试部署中，评估新的功能并将其部署于细心挑选的用户组。在先导测试部署过程中，多数用户还会继续使用旧的版本。

   假定先导测试部署成功，IT 人员即会将新软件在单位的其余部分实施。对旧的版本来说，有两种选择：

   - 强制升级。
   - 保留现有版本，但不提供支持。
3. 最终，所有用户将使用新的版本，几乎没有什么原因再让旧的应用程序继续流通。此时，您可能想将其从软件分发享中删除、备份，并将其存档以备将来需要时使用。

图 24.4 说明了这个过程。

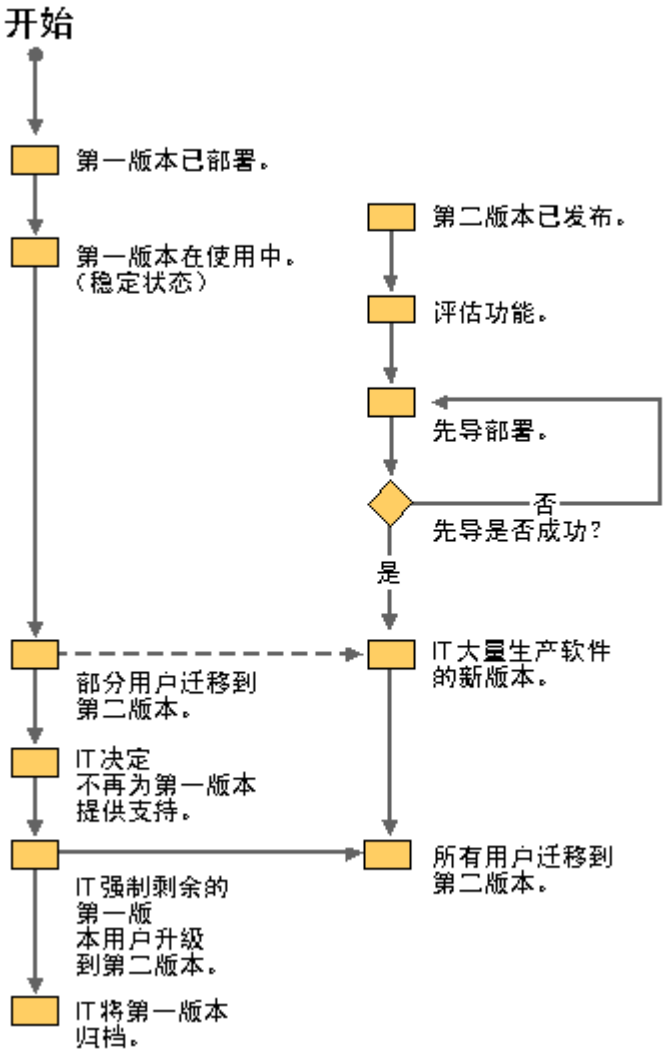


图 24.4 软件生命周期

软件的生命周期涉及以下软件管理任务：

- 安装
- 修改
- 升级
- 修复
- 删除

到目前为止，有关 IntelliMirror 软件安装和维护的讨论基本上完全集中于安装。下面的部分将讨论修改、升级和删除。

修补现有软件

软件发行者通常在应用程序中提供解决某一特定具体问题的补丁程序。需要决定您的单位是否需要这个补丁

程序。

如果决定部署 Windows 2000 的补丁程序，可以将补丁程序文件复制到软件分发点并替换旧的文件。分发补丁程序的软件发行者应提供新的 Windows 安装服务程序包（一个 .msi 文件）或 Windows 安装服务补丁程序（一个 .msp 文件）。使用 Windows 安装服务程序包，只需替换现有的程序包。或者可以使用 Windows 安装服务补丁程序对现有程序包作升级。

随后使用软件安装管理单元重新部署已指派或已发行的程序包。这使已打补丁或已升级的文件复制到已安装此软件的用户的计算机上。

服务包通常包含一些已经一起测试过的补丁程序。因此，服务包不象补丁程序分发地那么频繁，但是比完全升级还是要频繁些。

备注 如果某服务包只更新小数量的文件，可以如同对补丁程序那样对其分发和管理。如果某服务包更新大量文件，可以如同升级那样分发和管理。

升级现有软件

网络环境中有两种升级类型：

- **立即出现的强制升级。**这就是说安装了应用程序现有版本的用户会升级到新的版本，没有安装软件的用户只能安装升级版本。
- **不立即出现的非强制升级。**现有用户可以选择是否进行升级，新建用户可以自行决定安装何版本。

起初，您可能希望使新的升级是非强制性的，这样用户在想升级的时候才作升级。最终，您可能决定将非强制性升级改为强制性升级。

Windows 安装服务程序包是基于称为“公开的升级关系”的概念而建立的，即每个程序包都知道它能够为其他哪些程序包作升级。可以使用软件安装管理单元来创建这种公开的升级关系。例如，一个 Microsoft® Word 2000 程序包可以升级 Microsoft Word 6.0 和 Microsoft Word 7.0。

这一公开的升级关系需要原编的而非重新打包的应用程序。这就是说必须为重新打包的应用程序手动创建升级关系。

新的程序包（无论是原编的还是重新打包的）也许不能升级一个非原编的应用程序。在某些情况下，必须使用软件安装和维护来删除现有的应用程序，和用升级版本来替换。

也有可能完全删除重新打包的应用程序。某些组件，例如桌面快捷方式，即使没有被共享，也并不需要，可能也必须手动删除。随着更多的有原编程序包的应用程序的出现，升级可能会将现有的应用程序迁移到新的应用程序。

软件删除

在某一点上，几乎所有软件都不再需要了，需要决定如何处理它们。可以简单地停止提供支持，即便用户继续使用这过时的应用程序。那么就由用户到不再使用时删除它。另一方面，新的用户将不能从在“添加/删除程序”、“启动”菜单或通过文档调用来安装软件。

或者，可以从用户的计算机上强制执行软件的删除。要删除软件，在软件安装管理单元中选择软件包，然后在快捷菜单中单击“删除”。可以在用户下次登录时强制删除软件（在软件是已发行或是已指派给用户的情况下），或计算机下次重启时（在软件已指派给计算机的情况下）。现在可能不在办公室或正在休假的用户，只要在下一年中至少登录一次，就可以删除软件。

维护网络中的用户数据和设置

不论用户是否连接网络或使用哪台计算机，用户数据管理和用户设置管理使得数据和设置可以跟随用户。可以通过在网络服务器上、以及与此同步的本地硬盘的脱机位置存储相关信息，来增加用户对数据和他/她的个人环境的访问。

许多同样的技术用于实施用户数据和设置管理。尽管有些单位可能将数据和设置管理分开部署，其他单位会同时对他们进行规划和部署。以下部分将用户设置和用户数据管理放在一起讨论。

要中心管理用户数据和设置，需要以下的技术：

Active Directory 提供使用和管理组策略的基本架构。

组策略 允许系统管理员为用户或计算机自定义和控制 Windows 2000 元素，如桌面型计算机、网络访问以及 Microsoft® Internet Explorer。

漫游用户配置文件 使用户的个人设置和桌面配置，包括任何“开始”菜单自定义和“My Documents”文件夹的内容能够跟随他们从一台计算机到另一台计算机。这使他们能够无论使用哪台计算机，都拥有一个熟悉的工作环境。

文件夹重定向 使用组策略将个人文件夹（“My Documents”、应用程序数据、开始菜单以及桌面）重定向到网络服务器。当重新定向个人文件夹时，它将存储在网络上，无论用户从哪台计算机登录都可以使用。

脱机文件（或文件夹）允许用户维护文档的两个副本，一个存储在网络文件共享上，另一个在用户计算机上。每次用户登录或注销时，Windows 2000 同步文档的两个副本。

磁盘配额 限制用户在 NTFS 文件系统卷的存储信息量。由于多数 IntelliMirror 技术涉及在网络而不是本地硬盘上存储用户数据，可能需要磁盘配额以确保用户有足够的网络存储空间。

安全设置 允许任意访问控制表(DACLs)设置于文件和文件夹。

图 24.5 说明了启用用户数据和设置管理所需要完成的关键规划步骤。

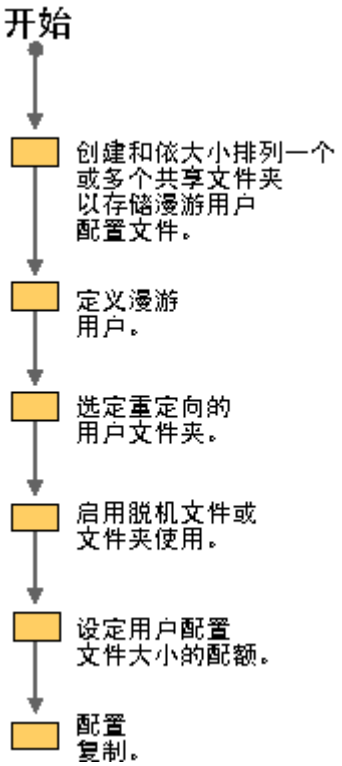


图 **24.5 用户数据和设置管理的规划步骤**

在以下部分，您将学到启用用户数据和设置管理所需的其他技术：

- 漫游用户配置文件
- 文件夹重定向
- 脱机文件（或文件夹）
- 同步管理器
- 磁盘配额

启用漫游用户配置文件

漫游用户配置文件为用户提供熟悉和易于使用的工作环境的方法。与存储在运行 Windows 2000 Professional 的单个计算机上的本地配置文件不同，漫游配置文件存储于网络共享，即可以通过网络上任何基于 Windows 2000 的计算机访问。

无论是本地的还是漫游的用户配置文件，都包含一些文件夹，包括但不仅限于应用程序数据、桌面、收藏夹、“ My Documents ”以及“ 开始 ”菜单。

一般而言，Windows 2000 中的漫游用户配置文件的实施与 Windows NT 4.0 的实施类似。有关类似点和不同点的详细信息，请参见 《Microsoft Windows 2000 Server Resource Kit Distributed Systems Guide》中的“ Introduction to Desktop Management ”。

设置漫游用户配置文件

1. 设置网络共享以在服务器上存储用户配置文件。
2. 将文件夹配置为共享文件夹。
3. 打开 Active Directory 用户和计算机管理单元，并导航到用户属性所在的特定节点。
4. 在用户名上单击鼠标右键，并单击快捷方式菜单上的“ 属性 ”。
5. 单击“ 配置文件 ”选项卡。
6. 在配置文件路径中输入存储用户配置文件的网络共享路径。例如网络名是 MaryK 的用户，\\NetworkShare\Profiles\MaryK 这个路径会在存储用户配置文件的服务器配置文件共享中创建一个名为 MaryK 的目录。

仅有存储于网络上的项目会漫游。即其他项目，例如屏幕保护程序和墙纸仅有在其副本存储于用户登录的每个计算机上时才可用。

设置漫游用户配置文件的指导方针

漫游用户配置文件既有优点，又有缺点。优点是个人设置和文件可以在用户更换计算机时跟随用户。潜在的缺点包括可能带来的网络流量。需要测试具体使用情况以确定单位合适的漫游支持层次。建议通过象电话线这样的低速连接访问网络的远程访问用户不使用漫游用户配置文件。

重定向文件夹

个人文件夹，包括“ My Document ”和“ My Pictures ”，可以使用组策略重定向。无论用户从哪台计算机登录，都可以使用已经重定向的文件夹。这样也易于系统管理员的管理和备份。

对用户来说，重定向的文件夹外观和操作都象本地存储的个人文件夹。重定向文件夹与包含漫游用户配置文件的文件夹不同，不在用户登录或注销网络时复制于整个网络。重定向文件夹可以让用户便利地访问他们的文档而不造成网络紧张。

要重定向文件夹，在组策略控制台中新建组策略对象，然后展开“ 用户配置 ”、“ Windows 设置 ”以及“ 文件夹重定向 ”。可以重定向的五个个人文件夹——“ 应用程序数据 ”、“ 桌面 ”、“ My Documents ”、“ My Pictures ”以及“ 开始 ”菜单的图标将是可见的。要重定向任何文件夹，在文件夹名上单击鼠标右键，单击“ 属性 ”，然后选择下列选项之一：

基本 将每个人的文件夹重定向到同一个网络共享点。此组策略对象所影响的所有文件夹会存储于同一个网络共享。

高级 基于用户在 Windows 2000 安全组的成员身份重定向个人文件夹。文件夹基于安全组成员身份重定向于不同的网络共享。例如，属于计帐组用户的文件夹可重定向于财务服务器，而销售组用户的文件夹可重定位于市场组的服务器。

当选择基本或高级设置时，必须输入共享文件夹名称，作为目标文件夹位置。例如：

*FolderServer**MyDocumentsFolders**Username*

在输入目标文件夹位置后，选择“ 设置 ”选项卡，在对话框中配置需要的选项，然后单击“ 完成 ”实现文件夹重定向。

备注 不要预先创建由“ 用户名 ”定义的目录。文件夹重定向将在文件夹上设置合适的 DACL。

配置文件夹重定向的指导方针

通过重定向文件夹，可以使用户能够按其需要使用文件。您也可以将文档包含在服务器备份计划中，以改进它们的可用性。

如果漫游用户配置文件造成单位太大的网络流量，考虑仅重定向有选择的个人文件夹，这样至少文件可以跟随用户在计算机之间移动，即便个人设置是不动的。

配置脱机文件的同步

多数单位已经开始备份过程，特别是对关键性的数据。在某些情况下，他们可能使用如 Systems Management Server 或第三方软件产品这样的程序来执行这一关键的任务。

在很多情况下，关键性的数据文件或文件夹由多个用户共享，例如现场销售队伍。保留所有这些文件或文件夹的当前版本是个严峻的 IT 问题。

Windows 2000 提供了同步管理器，能够更容易地确保客户计算机上和网络服务器上保留了关键文件和文件夹的当前版本，并且确保在进程中定期备份重要数据。

同步管理器对间断地连接网络的远程或旅行用户极有价值。使用同步管理器，可以控制何时将脱机用户的文件与网络上的文件同步。因为用户在脱机时和联机时访问文件的方式是完全一样的，所以此过程对用户是透明的。这确保需要时他们可以从网络上得到最新的信息，同时有助于将其本地计算机上的数据丢失引起的潜在破坏降到最低限度。

同步管理器将网络上的项目与用户脱机工作时打开或更新的项目进行比较，并使当前版本在本地计算机和网络上可用。可以同步的项目有单独文件、整个文件夹和脱机 Web 页。同步管理器可以在以下情况下自动同步脱机可用的信息：

- 每次用户登录或注销网络，或两者都可。
- 当计算机空闲但仍旧连接在网络上，以特定的间隔。
- 在计划的时间。

这些选项和不同选项的组合可用于不同共享资源的脱机文件。

系统管理员可指定脱机使用可用的任何共享网络文件夹。

标记脱机使用的共享文件夹

1. 在 Windows 资源管理器中，在要共享的文件夹上单击鼠标右键。
2. 单击“共享”，然后单击“缓存”。

   选定“此共享文件夹中允许文件缓存”，然后从以下设置中选择一个并单击“确定”。

   - **文档手动缓存。**用户必须手动指定想存储的文档。所有选定的文件将自动存储。
   - **文档自动缓存。**可以存储文件夹的整个内容。但是，只有用户实际打开的文件才能被存储。这样就比手动存储带来的网络通信少，因为手动存储时所有选定的文件，无论是否打开都会存储。
   - **程序自动缓存。**文档或程序的网络版本只存储一次，其后使用脱机版本，因而减少网络通信。

此设置是为包含只读文档的文件夹或为能从网络运行而设计的应用程序而设计的。

配置脱机文件的指导方针

组策略为您提供在本单位内管理脱机文件夹的许多方法：

首先，可以使用一个文件夹的共享/缓存选项决定在特定的客户计算机中脱机文件夹是否可用。当共享文件夹时，默认缓存模式设置为“ 对文档手动缓存 ”。为防止用户缓存文件夹，清除“ 此共享文件夹中允许文件缓存 ”复选框。

同样，可以使用“ 不缓存的文件 ”指定某些不缓存的文件类型（按扩展名）。例如，可以使用此选项防止大的 .avi 多媒体文件通过网络来回传输。

使用选项“ 禁止用户配置注销同步 ”，可以防止用户手动更改前面介绍的同步选项。

其它两个选项，“ 注销时自动同步 ”和“ 禁止用户同步文件夹和文件 ”，允许您控制同步发生的时间，而不控制将哪些文件同步。第一个选项指出在注销时执行的同步的类型——快速或完全。快速同步单独同步用户选择的文件。完全同步也自动同步缓存文件。“ 禁止用户同步文件夹和文件 ”允许指定只有在登录和注销时发生的同步。

设置磁盘配额

虽然让用户在网络上储存他们的文档和配置文件有一些优点，但可能一些用户使用服务器上所有可用的硬盘空间。可以配置磁盘配额以防止这种情况发生，并在用户对文件储存空间的需求与增加更多储存空间的花销之间平衡。

可以按每用户每卷设置磁盘配额。如果单个用户的配置文件超过预先确定的文件限制，那么在减小文件之前，该用户就不能注销计算机。每用户每卷配额有两个主要优点：

- 在卷上设置配额时，这些配额只对该卷有效。如果用户在好几个 NTFS 文件系统卷中储存文件，可以在每个卷上配置单独的配额。
- 配额由拥有文件的人付费。因此，所有权界线是分明的，即使用户与其他人共享一个或更多文件。

设置磁盘配额的指导方针

为用户的正当存储要求提供足够的磁盘空间，但不用让本单位添加不必要的服务器存放用户可以放置到网络共享中的所有文件是十分重要的。不用问用户自己他们需要多少网络磁盘空间，应考虑使用最初的先导测试部署计算出用户实际上需要多少网络存储的有用数据。

切记不是所有用户都有相同的存储要求。例如，软件开发人员比其他用户需要更大的网络存储。财务和工程用户是另外两个经常有比其他用户更大和更多文件的用户组。

为了为本单位设置有效的磁盘配额，在实施严格的配额之前弄清用户的合理要求是什么。

有关设置和使用磁盘配额的详细信息，参见本书中的“ 确定 Windows 2000 存储管理策略 ”。

为单位选择更改与配置管理选项

为准备更改与配置实现规划，必须确定哪些功能对于每个用户组的用处最大，如何对那些功能进行配置。

将本章介绍的更改与配置管理选项看作为用户提供更好服务的可部署组件。一些软件程序块可以为典型的单位提供基本支持，而另一些程序块提供更高级支持。

要完成 IntelliMirror 和远程 OS 安装规划：

- 定义哪些功能用于基本更改与配置管理和哪些功能用于高级更改与配置管理。
- 定义基本和高级更改与配置管理选项如何才能最佳地满足本单位用户类型的需求。
- 概述更改与配置管理将如何满足本单位的需求。

下面几节是如何在更改与配置管理规划中实现 IntelliMirror 和远程 OS 安装功能的示例。根据您的需求的不同，在下面几节作为高级选项列出的一些选项可能对您的单位来说实际上是基本选项，而作为基本选项列出的一些选项可能对另一个单位却是高级选项。必须为本单位定义基本和高级要求和实施方法。

基本和高级选项的概述

下列使用选项适用于基本用户数据管理要求：

- 给用户提供专用网络共享并将他们的 My Documents 文件夹映射到此共享。
- 将桌面作为此网络共享的组成部分，以使保存到桌面的文档同时也保存到网络共享中。
- 给用户提供公用网络共享。此共享可以为单个用户或工作组服务。
- 在共享中设置配额，特别是在每用户共享中。
- 为共享，特别是为每用户共享提供备份和恢复服务。
- 在包含专用数据共享中启用脱机文件夹。
- 对一般数据类型启用同步管理器。

对于高级用户数据管理，应考虑实施下列功能：

- 对于使用多个本地计算机的用户实施漫游用户配置文件。
- 保证当漫游用户离开计算机时，漫游用户的配置文件和缓存都被清除。

对于基本设置管理，应考虑提供下列选项：

- 为桌面或外壳控制建立基本策略。
- 为安全性控制建立基本策略（参见本书的“ 网络安全规划 ”）。
- 定义登录脚本。
- 不能将多于五或六个组策略对象应用到一个给定用户和计算机。（有关使用并应用组策略到管理客户配置的详细信息，参见本书的“ 定义客户管理与配置标准 ”）。
- 对于漫游用户配置文件的用户，为新用户定义标准默认用户配置文件。此默认配置文件存在服务器上并在用户第一次登录时被复制到的计算机。

对于高级设置管理，应考虑提供下列选项：

- 配置组策略以严格限制对系统文件位置的访问。
- 配置组策略以防止用户运行未经批准的软件。

对于基本软件安装和维护，应考虑使用下列选项：

- 允许用户在应用程序的使用周期内使用“ 添加/删除程序 ”。
- 防止用户使用 CD 安装软件。
- 以“ 部分安装/按需安装 ”的形式发行现有的基于 Windows 安装服务的应用程序。
- 使用转换修改软件包操作。
- 发行或指派操作系统更新。
- 使用组策略升级应用程序。

对于高级软件安装和维护，应考虑使用下列选项：

- 创建启用 Dfs 的分发点。
- 使用 Systems Management Server 管理 Dfs 分发点。

下面几节阐明一些不同类型的用户的更改与配置管理规划。

满足技术用户的需求

技术用户（如开发人员）常常必须是他们自己计算机的管理员。他们通常希望 IT 部门提供管理服务，而又不剥夺他们控制自己计算机的能力。

对于这些用户，Windows 2000 更改与配置管理可以帮助简化他们计算机的安装，并把个人数据丢失降到最低。

下列基本和高级选项阐明如何对技术用户应用更改与配置管理：

- **基本用户数据管理。**所有方面都适用。重定向 My Documents，特别是为膝上型电脑用户。不要重定向桌面。在 My Documents 共享中启用脱机文件夹。
- **高级用户数据管理。**一些技术用户可能想使用漫游用户配置文件。他们也想维护本地管理特权。
- **基本设置管理。**尽可能少地对他们的配置实施覆盖。
- **高级设置管理。**无
- **基本软件安装和维护。**所有方面都适用。发行的应用程序和远程 OS 安装具有很强的优点，但不会剥夺技术用户的控制。
- **高级软件安装和维护。**无指派或任何形式的控制。
- **高级远程 OS 安装。**授予高级安装选项的访问权限。若有必要，使所有可应用的安装映像可供用户选择。

满足固定专业用户的需求

固定专业用户通常喜欢一些管理服务——只要它们能增值并不需要太多的配置控制。

对于这些用户，远程 OS 安装和 IntelliMirror 提供安装他们计算机的最简单方法，以及提供数据备份和为最普通的使用提供最佳功能组合。

下列基本和高级选项规划阐明如何对固定专业用户应用更改与配置管理：

- **基本用户数据管理。**所有方面都适用。桌面可以重定向。本地专用存储是这组的好的选项。
- **高级用户数据管理。**一些用户可能想要漫游用户配置文件。使用加密文件系统可能对于高级经理人员有吸引力。然而，注意加密文件和文件夹不能包含在漫游用户配置文件中。然而，加密文件和文件夹也可以重定向。
- **基本设置管理。**有限数量的覆盖是可以忍受的。这些用户不能充当本地管理员。
- **高级设置管理。**控制计算机状态和存取是没有问题的。然而，如果基于网络的配额很少，这常常需要创建本地 My Documents 文件夹。
- **基本软件安装和维护。**所有方面都适用，包括应用程序发行。对于可选功能使用按需安装。
- **高级软件安装和维护。**谨慎地使用应用程序指派。
- **基本远程 OS 安装。**通过限制安装选项和可用的映像，尽可能地简化过程。

满足漫游专业用户的需求

漫游专业用户与固定专业用户非常类似。即使他们使用多个计算机，他们通常也有一台主要计算机。

对于这些用户，漫游应该不费力气，不应产生固定使用以外的费用。

下列规划阐明如何对漫游专业用户应用基本和高级更改与配置管理：

- **基本用户数据管理。**所有方面都适用。本地专用存储对于这组是基本的。桌面应该重定向。
- **高级用户数据管理。**要求漫游用户配置文件。使用加密文件系统可能对于高级经理人员有吸引力。然而，注意加密文件和文件夹不能包含在漫游用户配置文件中。然而，加密文件和文件夹可以重定向。
- **基本设置管理。**有限数量的覆盖是可以忍受的。他们不是本地管理员。
- **高级设置管理。**控制计算机状态和存取是没有问题的。然而，如果基于网络的配额很少，这常常需要创建本地 My Documents 文件夹。
- **基本软件安装和维护。**所有方面都适用。可使用应用程序发行，但只有当您可以从网络运行应用程序以使应用程序不必安装在本地计算机时才可使用。对于可选功能使用按需安装。
- **高级软件安装和维护。**谨慎地使用应用程序指派。只对用户、只对计算机、不对计算机指派应用程序。
- **基本远程 OS 安装。**所有用户访问远程安装选项被完全删除，以使所有安装都由管理人员或者帮助中心人员执行。或者，远程安装选项受到限制以使安装完全自动。

满足移动专业用户的需求

移动用户从 Windows 2000 新功能中获益颇多，如同步管理器、加密文件系统、客户端缓存，和即插即用。

这些用户通常使用膝上型电脑以及主要的台式机。

下面阐明如何对移动专业用户应用更改与配置管理：

- **基本用户数据管理。**所有方面都适用。桌面不应该重定向。本地专用存储对于这组是基本的。重定向和脱机文件夹对于是这组的理想选项。
- **高级用户数据管理。**通常使用漫游用户配置文件。然而，如果用户只有一台计算机，那么不要求漫游用户配置文件，除非可能出于数据保护的需要。必须使用加密文件系统。
- **基本设置管理。**有限数量的覆盖是可以忍受的。他们不是本地管理员。
- **高级设置管理。**由于用户与管理员的距离，用户常常对膝上型电脑有较大的控制。
- **基本软件安装和维护。**所有方面都适用。可使用应用程序发行，但只有当您可以本地安装应用程序时才行。对于可选功能不使用按需安装。
- **高级软件安装和维护。**可以指派应用程序，但只有当它们本地安装时才行。当用户与软件分发点断开连接时允许他们从本地资源（如 CD）安装。
- **高级远程 OS 安装。**支持便携式计算机进行远程 OS 安装，但只有当它们通过包含远程引导 ROM 的插接站或通过支持的网卡连接到网络才行。对于不靠接或很少靠接的用户允许使用远程安装，应考虑操作系统重新安装的替换方案或步骤。

满足基于任务的用户的需求

基于任务的用户通常没有他们自己的计算机。当他们注销计算机时，没有必须留下的计算机设置数据文件。这些用户不能安装任何应用程序、在他们的网络共享之外创建文件，或改变本地计算机管理员配置的状态。在某些情况下，这些计算机可能是 Windows 终端服务客户。

下面阐明如何对基于任务的用户应用更改与配置管理：

- **基本用户数据管理。**所有方面都适用于非 kiosk 样式的环境。桌面重定向。没有本地存储。对于 kiosk，当用户注销时，本地配置文件被删除。
- **高级用户数据管理。**只有当这是非 kiosk 样式的环境时才使用漫游用户配置文件。没有数据应该留下。
- **基本设置管理。**桌面重定向。计算机设置严格受到控制。
- **高级设置管理。**桌面重定向。计算机设置严格受到控制。
- **基本软件安装和维护。**大多数应用程序基于计算机（而不是用户）安装。在需要对用户指派应用程序时，应从网络运行。
- **高级软件安装和维护。**只指派应用程序。禁止从网络以外的任何地方安装软件。
- **基本远程 OS 安装。**访问远程安装选项被完全删除，以使安装只能由管理人员或者帮助中心人员执行。或者，安装选项受到限制以使操作系统安装自动执行。

摘要

表 24.6 列出了有多种类型用户的大单位的更改与配置管理策略示例。

表 24.6 更改与配置管理策略示例

用户分类	用户数据管理	用户设置管理	软件安装与维护	远程 OS 安装
技术用户	基本	基本（没有锁闭）	基本	高级
固定专业用户	基本	基本	高级	基本
漫游专业用户	高级	基本	高级	基本
移动专业用户	高级	基本	高级	高级
基于任务的用户	高级	高级	高级	基本

对于用户数据管理，遵循下列指导方针：

- 基本用户数据管理对只适度地管理客户计算机的公司有用。
- 高级用户数据管理取决于用户的类型，特别是在高度管理的环境中，和保证高层次的服务时（例如，对于资深经理）。

对于用户设置管理，应用下列指导方针：

- 基本设置管理主要用于适度管理客户计算机的单位，而且最常用于被高度管理的客户计算机。当有专职管理人员在场时使用最为频繁。
- 高级设置管理主要用于支持费用紧张的高度管理的环境中，如学校、医院和工厂。

对于软件安装和维护，应用下列指导方针：

- 基本软件安装和维护将变成标准做法，特别是单位软件的发行。
- 高级软件安装和管理主要用于支持费用紧张的高度管理的环境中，如学校、医院和工厂。

对于远程操作系统安装，应用下列指导方针：

- 当用户选项受到限制或高度自动化时，使用基本远程操作系统安装。如果允许用户执行远程安装，他们只需在系统启动时启动远程安装并输入用户名和密码。
- 当用户可以选择安装哪些操作系统映像以及如何安装、或特殊的情况保证用户进行安装具有更高的灵活性时，使用高级远程操作系统安。

更改与配置管理规划任务列表

表 24.7 总结了制定 Windows 2000 更改与配置管理规划必须执行的任务。

表 24.7 更改与配置管理规划任务列表

任务	所在章节
定义用户和单位更改与配置管理需求。	评估更改与配置管理
评估和选择想要的 Windows 2000 更改与配置管理功能。	评估更改与配置管理
使用远程 OS 安装安装 Windows 2000 的规划。	启用远程 OS 安装
配置组策略以启用 IntelliMirror 软件安装和维护。	使用组策略改善软件管理
为用户数据管理配置服务器共享和组策略。	维护网络中的用户数据和设置
为用户设置配置服务器共享和组策略。	维护网络中的用户数据和设置

第 25 章 - 客户机自动安装与升级

现在，您已准备好开发并执行 Microsoft® Windows® 2000 Professional 及相关应用程序的自动安装了。这是执行任何级别部署的先决条件：包括测试、先导测试或生产应用。本章介绍了可用的自动安装方法，包括准备需求和示例配置。建议参与安装进程设计的网络工程师和参与安装 Windows 2000 及相关应用程序的系统管理员熟悉本章内容。

安装 Windows 2000 Professional 包括：在未安装过 Microsoft Windows 2000 之前操作系统的电脑上执行全新安装，或者在目前运行 Microsoft® Windows® 95、Microsoft® Windows® 98、Microsoft® Windows NT® Workstation 3.51 版或 Microsoft® Windows NT® Workstation 4.0 版的电脑上执行全新安装和升级。在决定进行全新安装或者升级之前，需要解决在本书“规划概述”中讨论的一些关键性规划问题。

本章内容

确定进行升级还是执行全新安装
安装的准备工作
自动安装客户机应用程序
自动安装 Windows 2000 Professional
安装配置示例
安装任务列表

本章目标

本章将帮助您完成以下规划文档：

- 自动安装规划

资源工具包中的相关信息

- 关于规划的详细信息，请参见本书“规划概述”一章。
- 关于服务器自动安装的详细信息，请参见本书中的“服务器自动安装与升级”。
- 关于管理客户机的详细信息，请参见本书中的“定义客户管理与配置标准”。
- 关于本章引用的自动安装参数的详细信息，请参阅 Microsoft Windows 2000 操作系统 CD 中的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，可用 Windows 资源管理器找到该文件。在 Windows 95 及早期版本或在 MS-DOS® 中，可用 **Extract** 命令访问该文件。
- 有关无人参与安装的详细信息，包括应答文件示例，请参见本书附录“无人参与安装的应答文件示例”。

确定进行升级还是执行全新安装

在企业环境中，如果在每台计算机上均用标准的交互式设置来安装 Windows 2000，其性能价格比是不理想的。要大幅度降低总体拥有成本 (TCO)，可以在多台计算机上都执行 Windows 2000 Professional 自动安装。

	关键决定 在执行 Windows 2000 Professional 的自动安装之前，必须确定该安装是从 Windows NT 升级还是进行全新安装。

下列两项将会有助于确定是升级还是进行全新安装。

- 如果组织已应用了 Windows 操作系统，并且对信息技术 (IT) 部门实行集中管理，则有可能会希望进行升级。如果正筹建一个目前组织中不存在的受管理环境，则会希望执行全新安装，这样，即可在安装时实施标准配置。
- 如果打算使用现有的硬件和软件应用程序，则需要进行升级。相反，如果计划购买新硬件并安装新的软件应用程序，则需要执行全新安装。

解决关键规划问题

显然，如果打算在未安装 Windows 2000 以前操作系统的计算机上安装 Windows 2000 Professional，则应选择进行全新安装。如果计算机目前正运行 Windows 95、Windows 98、Windows NT Workstation 3.51 或 Windows NT Workstation 4.0，则需确定升级现有操作系统和进行全新安装哪个更为合算。

表 25.1 总结了一般性的规划问题

表 25.1 升级或安装之前要解决的规划问题

问题	任务
组织目标	定义公司的主要目标。
区域需求	表明具体的区域需求，并确定业务是否会包括国际分支机构或公司。
用户组	分析用户组，包括具体的职位类别和需求、用户的计算机知识与经验、安全性需求、用户位置，以及包括链接速度在内的网络连接问题。
应用程序需求	确定哪些产品将预先安装到所有计算机中，哪些产品发布给特定的用户，而又有哪些产品分发给特定的用户类型。
计算机/用户策略	评估现有数据存储和用户设置；确定用户设置的迁移需求；评估必需的、漫游的和本地的用户配置文件。
硬件	编制现有硬件的清单，确定对新硬件的需求。 升级或安装之前设置最低的硬件需求。 为将来的计算机需求作准备。 确定计算机在组织中如何循环。 确定是否所有计算机都有引导 CD-ROM。
风险和问题范围	确定潜在风险，包括应用程序与 Windows 2000 的不兼容

	性、时间限制问题、多个站点、非集中化预算，以及可能到来的合并的影响。
增长期望值	标明一年、三年和五年内的项目增长期望值。当获悉一些计划好的兼并、新站点、国家等问题时，必须对其加以说明。
网络问题	确定远程站点是否有应用程序部署服务器。确定中央站点以外的服务器如何升级。
软件管理	确定软件管理系统（如 Microsoft® Systems Management Server (SMS)）是否已就绪，以便规划部署。
连接	确定服务器及服务器之间的连接是否设置成给公司的所有人分发大型软件包。

选择安装方法

解决关键的规划问题之后，就可以选择自动安装的方法了。表 25.2 列出了自动安装的方法，并显示这些方法是可用于升级、全新安装，还是两种方式都可以。

表 25.2 自动安装方法

方法	Windows 2000 版本	升级	全新安装
Syspart	Server 和 Professional	否	是
Sysprep	Server 和 Professional	否	是
SMS	Server 和 Professional	是	是
引导 CD-ROM	Server 和 Professional	否	是
远程操作系统安装	Professional	否	是

准备安装

要为 Windows 2000 Professional 全新安装做准备，需做以下工作:

- 创建分发文件夹
- 了解如何使用应答文件
- 了解 Windows 2000 安装命令

备注 本节所述的执行自动安装原则对全新安装和升级都适用。最常见的情况是执行全新安装。

图 25.1 是显示安装过程的流程图。

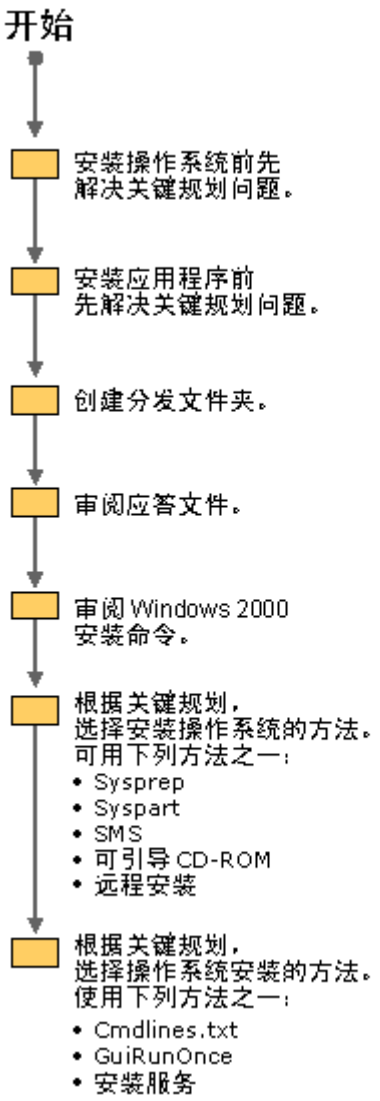


图 25.1 自动安装流程图

创建分发文件夹

要在网络的多个计算机上安装 Windows 2000 Professional，必须创建至少一套分发文件夹。分发文件夹一般驻留于与计算机相连接的服务器中，通过运行 Winnt.exe 或 Winnt32.exe，即可在目标计算机上安装 Windows 2000。针对不同的系统实施，可使用带有不同应答文件的同一套分发文件夹。即便使用磁盘映射作为安装方法，以分发文件夹做为开始也可以为不同的系统类型提供一致的执行方法。另外，您还可以通过编辑分发文件夹中的文件，或修改应答文件生成新的映像，来更新将来的映像，而无需再从头开始。

为了帮助平衡服务器负载，同时使运行 Windows 95、Windows 98、Windows NT 或 Windows 2000 的计算机在安装 Windows 2000 过程中，更迅速地完成文件复制阶段，您可在多个服务器上创建分发文件夹。然后就可以在最多八个源文件位置同时运行 Winnt32.exe。有关多个计算机上 Professional 的详细信息。

	重要决定 在执行 Windows 2000 Professional 的自动安装之前，必须先确定该安装是从 Windows NT 的升级还是全新安装。

以下两项将帮助您确定安装命令，请参见本章后面的“检查 Windows 2000 安装命令”。

备注　本章中，“Windows NT”一词既指 Microsoft Windows NT 3.51 也指 Microsoft Windows NT 4.0。

分发文件夹包括 Windows 2000 Professional 安装文件，以及安装时需要的任何设备驱动程序和其他文件。

Setup Manager 是 Windows 2000 Professional CD 提供的工具，可为您提供帮助，使分发文件夹的创建过程自动化。有关 Setup Manage 的详细信息，请参见本章后面的“创建应答文件”。

备注 在本章中，“Windows 2000 安装”也称为“安装”。

要创建一个分发文件夹：

1. 连接到要在上面创建分发文件夹的网络服务器。
2. 在网络服务器的分发共享上创建一个 \i386 文件夹。

   要帮助区分不同版本 Windows 2000 (Microsoft Windows 2000 Professional、Microsoft® Windows® 2000 Server 和用于 Microsoft® Windows® 2000 Advanced Server 的一个版本)的多个分发共享，您可为这个文件夹选择其他名称。如果组织的跨国分部准备使用 Windows 2000 的本地化语言版本，则可为每个本地化版本都创建单独的分发共享。
3. 将 \i386 文件夹的内容由 Windows 2000 Professional CD 复制到已创建的文件夹中。
4. 在所创建的文件夹中，创建名为 OEM 的子文件夹。

   安装过程中，OEM 子文件夹会为要复制到目标计算机上的附加文件提供必要的文件夹结构。这些文件包括驱动程序、实用工具、应用程序和任何其他在组织内部署 Windows 2000 Professional 时所需的文件。

构建分发文件夹

图 25.2 显示了分发文件夹的一个样本结构。

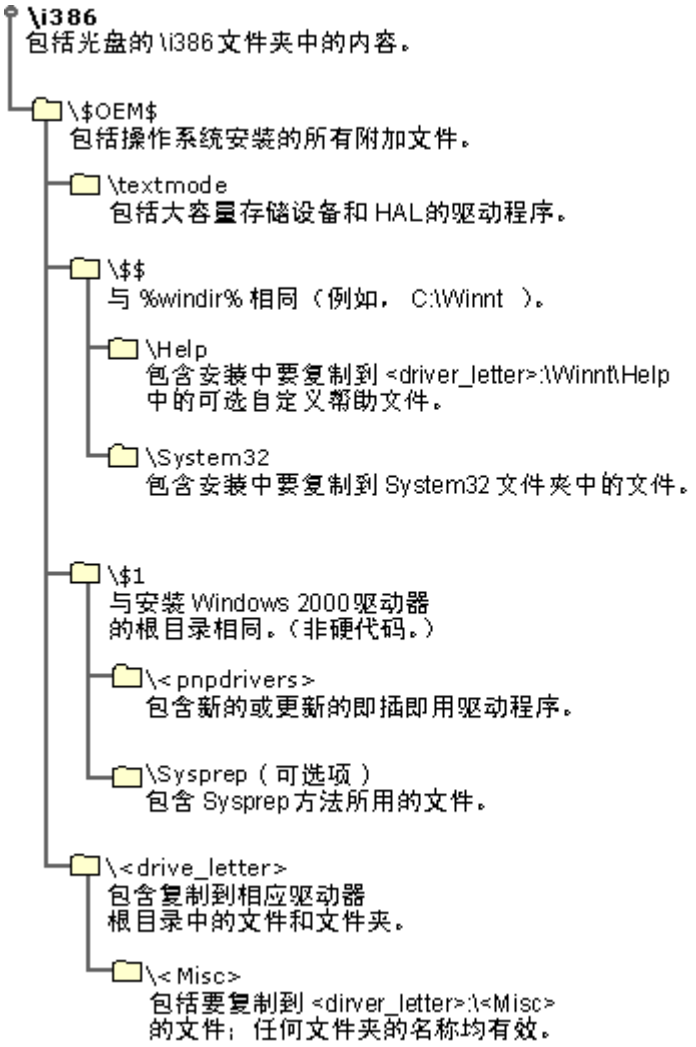


图 25.2 分发文件夹的结构示例

i386

这是分发文件夹，包含了安装 Windows 2000 所需的所有文件。通过把 Windows 2000 Server CD 中的 i386 文件夹的内容复制到分发文件夹中，就在分布式共享的根目录下创建了此文件夹。

OEM

应直接在分发文件夹的 i386 文件夹下面创建 OEM 子文件夹。安装过程中，您可以把目录、标准 8.3 格式文件以及任何自动安装过程所需的工具自动地复制到 OEM 子文件夹中。

备注　如果在应答文件中使用了 OEMFILESPATH 关键字，就可以在分发文件夹之外创建 OEM 子文件夹。有关应答文件定义的详细信息，请参见本章后的“检查应答文件”。关于应答文件参数和语法的详细信息，请参阅 Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，可使用 Windows 资源管理器找到这个文件。在 Windows 95 及早期版本，或在 MS-DOS 中，可用 **Extract** 命令访问该文件。

OEM 子文件夹可以包含可选文件 Cmdlines.txt，该文件包含了安装程序的图形用户界面 (GUI) 部分所要运行的命令列表。这些命令可用于安装您想在安装中包括的其他工具。有关 Cmdlines.txt 文件的详细信息，请参见本章后面的“使用 Cmdlines.txt”。

安装程序一旦在分发点根目录下找到 OEM 子文件夹，就会把在这个目录下发现的所有文件复制到一个临时目录，该目录是在安装过程的文本部分创建的。

备注 本章中，安装程序的 GUI 部分称做“ GUI 模式 ”，安装程序的文本部分称做“ 文本模式 ”。

OEM\textmode

OEM\textmode 子文件夹包含了安装大型存储设备驱动程序和硬件抽象层 (HAL) 使用的新建或已更新的文件。这些文件可能包括 OEM HAL、小型计算机系统接口 (SCSI) 设备驱动程序及引导这些组件的加载和安装的 Txtsetup.oem 文件。

确保包括 Txtsetup.oem 文件。OEM\textmode 子文件夹中的所有文件（HAL、驱动程序和 Txtsetup.oem）必须在应答文件的 [OEMBootFiles] 节列出。

OEM\$$

OEM\$$ 子文件夹与 %systemroot% 或 %windir% 环境变量对应。子文件夹包含要复制到 Windows 2000 安装目录的各个子文件夹上的其他文件。该子文件夹的结构必须与标准的 Windows 2000 安装结构相符，其中，OEM\$$ 对应 %systemroot% 或 %windir%（例如 C:\Winnt），OEM\$$\System32 对应 %windir%\System32，依次类推。每个子文件夹都必须包含要复制到目标计算机相应系统文件夹中的文件。

OEM\$1

OEM\$1 对 Windows 2000 而言是一个新的子文件夹，它指向安装了 Windows 2000 的驱动器。$1 相当于 %systemdrive% 环境变量。例如，如果正在 D 驱动器上安装 Windows 2000，则 OEM\$1 就指向 D 驱动器。

OEM\$1*PnPDrvs*

OEM\$1\Pnpdrvrs 子文件夹对 Windows 2000 而言也是新的，可使用该子文件夹，在分发文件夹中放置新的或更新过的即插即用设备驱动程序。这些文件夹将复制到目标计算机中的 %systemdrive%*Pnpdrvrs* 位置。如果把 OemPnPDriversPath 参数添至应答文件，就可以引导 Windows 2000 在您创建的文件夹中寻找（在安装过程中或安装之后）新的或是更新过的即插即用驱动程序，以及系统原有的驱动程序。请注意，可用自己的八个或少于八个字符的名称替代 *Pnpdrvrs*。

OEM\$1\Sysprep

OEM\$1\Sysprep 子文件夹是可选的。该子文件夹包含运行 Sysprep 工具所需的文件。有关 Sysprep 的详细信息，请参见本章后面的“ 使用 Sysprep 复制磁盘 ”。

OEM*drive_letter*

在文本模式中，每个 OEM*Drive_letter* 子文件夹的结构均会复制到目标计算机相应驱动器的根目录上。例如，放在 OEM\D 子文件夹中的文件会复制到 D 驱动器根目录。还可以在这些子文件夹中创建子文件夹。例如，OEM\E\Misc 使安装程序在 E 驱动器上创建一个名为 Misc 的子文件夹。

要重新命名的文件必须在 $$Rename.txt 中列出。关于重新命名文件的详细信息，请参阅本章后面的“ 使用 $$Rename.txt 转换文件名长度 ”。请注意，分发文件夹中的文件必须有使用 8.3 命名格式的短文件名。

安装大型存储设备

在 Windows 2000 中，即插即用会检测并安装大部分硬件设备，这些设备可在安装后再加载。然而，要在 GUI 模式中能够使用完整的即插即用支持，则必须正确安装大型存储设备，如硬盘。

备注 如果 Windows 2000 已对一个设备提供了支持，就不需要对其加以特殊指定。

要在文本模式阶段安装 SCSI 设备—即在完全的即插即用支持可用之前—您必须提供一个 Txtsetup.oem 文件，描述安装程序如何安装特定的 SCSI 设备。

重要提示 在使用更新的驱动器之前，要验证它们是否已签过名。如果尚未签名，安装会失败。可在设备管理器中检查单个驱动器的签名状态，或者运行 Sigverif.exe，以便在 %windir% 子文件夹中生成一个 Sigverif.txt 文件。Sigverif.txt 会列出系统中所有驱动器的签名状态。

要安装大型存储设备：

1. 在分发文件夹的 OEM 子文件夹中创建 Textmode 子文件夹。

   将以下文件复制到 Textmode 子文件夹中，这些文件可由设备供应商处获得（用适当的驱动器名称代替 *Driver* 这个词）：

   - *Driver.sys*
   - *Driver.dll*
   - *Driver.inf*
   - Txtsetup.oem

   备注 某些驱动器，如 SCSI 小型端口驱动器，可能不包括 .dll 文件。

2. 在应答文件中创建 [MassStorageDrivers] 节，并在该节中键入要包括的驱动器项目。例如，[MassStorageDrivers] 节的一个项目可能是 ：

   ```
   "Adaptec 2940Y" = "OEM"
   ```

   该节的信息可从 Txtsetup.oem 文件获得，该文件可由硬件制造商提供。

   关于应答文件参数和语法的详细信息，请参阅 Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，可用 Windows 资源管理器找出这个文件。在 Windows 95 及早期版本，或在 MS-DOS 中，可用 **Extract** 命令访问该文件。

3. 在应答文件中，创建 [OEMBootFiles] 节，并在该节键入 OEM\Textmode 文件夹的文件列表。例如，[MassBootFiles] 节的一个项目可能是 ：

   ```
   [OEMBootFiles]
   Driver.sys
   Driver.dll
   Driver.inf
   Txtsetup.oem
   ```

   其中的 *Driver* 是驱动器名。

4. 如果大型存储设备是即插即用设备，则 Txtsetup.oem 文件中会有一个名为 [HardwareIds.Scsi.yyyyy] 的节。如果大型存储设备没有这样一节，就需要创建一个并在其中键入以下项目：

   ```
   "xxxxx" , "yyyyy"
   ```

此处 *xxxxx* 代表设备标识符 (ID)，而 *yyyyy* 代表与该设备相关的服务。

例如，要安装设备识别符 (ID) 为 PCI\VEN_1000&DEV_0001 的 Symc810 驱动程序，须验证 Txtsetup.oem 文件是否包含以下附加节：

```
[HardwareIds.scsi.symc810]
id = "PCI\VEN_1000&DEV_0001" , "symc810"
```

安装硬件抽象层

要指定安装的硬件抽象层(HAL)，需要 Txtsetup.oem 文件和 HAL 文件（由供应商提供）。如果正在安装大型存储设备驱动程序，就必须使用与之相同的 Txtsetup.oem 文件。因为只可使用一个 Txtsetup.oem 文件，所以，若要安装 HAL 和大型存储设备驱动器，则需将项目合并到一个文件中。

要使用第三方驱动器，必须对应答文件进行适当的更改。有关应答文件参数和语法的详细信息，请参见 Microsoft Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，可用 Windows 资源管理器找出这个文件。在 Windows 95 及早期版本，或在 MS-DOS 中，可用 **Extract** 命令访问该文件。

要安装 HAL：

1. 如果尚未在 OEM 文件夹中创建 Textmode 子文件夹，请先创建该子文件夹。
2. 把从设备供应商处收到的文件复制到 Textmode 子文件夹中。
3. 在应答文件中，编辑 HAL 的 [Unattend] 节，并添加任何要安装的驱动程序。例如，可键入如下项目：

   ```
   [Unattend]
   Computertype = "HALDescription ", OEM
   ```

   HALDescription 的信息可以从 Txtsetup.oem 文件的 [Computer] 节获得，该文件由驱动程序供应商提供。
4. 在应答文件中，创建一个 [OEMBootFiles] 节，并输入 OEM\Textmode 文件夹中的文件名。

安装即插即用设备

以下步骤说明如何安装一些既非大型存储设备或 HAL，又不包括在 Windows 2000 操作系统 CD 上的即插即用设备。

要安装即插即用设备：

1. 在分发文件夹中创建子文件夹，专门用于特殊的即插即用驱动器及其 .inf 文件。例如，可以创建一个名为 PnPDrvs 的文件夹：

   ```
   $OEM$\$1\PnPDrvs
   ```
2. 在 Unattend.txt 文件中添加下行，以添加指向即插即用驱动程序搜索列表的路径。

   ```
   OEMPnPDriversPath = "PnPDrvs"
   ```

   如果 PnPDrvs 文件夹中有子文件夹，则必须指定每个子文件夹的路径。路径必须以分号隔开。

要使文件夹便于维护，以便适应将来的设备驱动程序，则要为可能的设备驱动程序创建子文件夹。把文件夹分成子文件夹，这样就可以按设备类型来存储设备驱动程序文件，而不是把所有设备驱动程序文件都放在同一个文件夹中。推荐的子文件夹包括 Audio、Modem、Net、Print、Video 和 Other。Other 文件夹可使您更灵活地存储可能目前未知的新硬件设备。

例如，如果 PnpDrvs 文件夹包含子文件夹 Audio、Modem 和 Net，那么应答文件必须包含如下的行：

```
OEMPnPDriversPath = "PnPDrvs\Audio;PnPDrvs\Modem;PnPDrvs\Net"
```

使用 $$Rename.txt 转换文件名长度

安装过程中，$$Rename.txt 文件会将短文件名改为长文件名。$$Rename.txt 列出了特定文件夹中所有要重新命名的文件。每个包含应重新命名短文件名的文件夹都必须有自己的 $$Rename.txt 版本。

要使用 $$Rename.txt，请把文件放入包含需要转换文件的文件夹。$$Rename.txt 的语法如下：

```
[section_name_1]
short_name_1 = "long_name_1"
short_name_2 = "long_name_2"


short_name_x = "long_name_x"

[section_name_2]
short_name_1 = "long_name_1"
short_name_2 = "long_name_2"


short_name_x = "long_name_x"
```

参数定义如下：

section_name_x：包含这些文件的子文件夹路径。如某节需要命名，它会有反斜线（\）作为名称，表示该节包含在驱动程序根目录上的文件或者子文件夹的名称。

short_name_x 该子文件夹中要重命名的文件或子文件夹名称。该名称不能加引号。

long_name_x 文件或子文件夹的新名称。如果该名称包含空格或逗号，则必须加引号。

提示 如果使用 MS-DOS 开始安装，且基于 MS-DOS 的工具无法复制路径名称多于 64 个字符的文件夹，就可以使用短文件名，然后用 $$Rename.txt 重新命名它们。

检查应答文件

应答文件是不需用户输入就可回答安装问题的自定义脚本。Windows 2000 Server CD 包含一个示例应答文件，您可对其加以修改并使用。应答文件通常以 Unattend.txt 命名，也可重新命名。（例如，只要已在 Setup 命令中正确指定了这些名称，Comp1.txt、Install.txt 和 Setup.txt 就都是有效的应答文件名。）如果要为所在组织的不同部分维护不同的脚本安装，则可重新命名应答文件，这样就能够创建和使用多个应答文件。请注意，其他程序也可使用应答文件，例如 Sysprep，它使用可选的 Sysprep.inf 文件。

应答文件会“告诉”安装程序如何与已创建的分发文件夹和文件进行交互。例如，在应答文件的 [Unattend] 节中有一个“OEMPreinstall”项目，它会提示安装程序把 OEM 子文件夹由分发文件夹复制到目标计算机上。

应答文件包含多个可选节，您可以修改它们，以提供与安装需求有关的信息。应答文件会在一个标准的互动式 Windows 2000 安装过程中，为安装程序提供所有问题的答案。Unattend.doc 文件包含与应答文件的关键字和值有关的详细信息。关于应答文件节及其相关参数的详细信息，请参见 Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，可用 Windows 资源管理器找到这个文件。在 Windows 95 及早期版本，或在 MS-DOS 中，可用 **Extract** 命令访问该文件。

要执行 Windows 2000 Server 无人参与安装，必须先创建一个应答文件；并在安装开始时，通过可引导方法，或运行 Winnt.exe 或 Winnt32.exe 来指定该文件。 以下是一个使用 Winnt.exe 的 Setup 命令示例:

```
Winnt /S:Z:\I386 /U:Z:\unattend.txt
```

请注意 **/U** 命令行开关，它表示无人参与安装。有关 Winnt.exe 和 Winnt32.exe 的详细信息，请参见本章后面的“检查 Windows 2000 安装命令”。

创建应答文件

应答文件是一个自定义脚本，可用它来运行 Windows 2000 Professional 的无人参与安装。有两种办法创建应答文件：既可用 Setup Manager 创建该文件，也可手动创建。

用 Setup Manager 创建应答文件

Windows 2000 操作系统 CD 的 \Support\Tools 文件夹中的 Deploy.cab 文件提供了 Setup Manager 应用程序，可帮助您创建或修改应答文件，使用 Setup Manage 可以提高创建或更新应答文件过程的一致性。

有关应答文件参数和语法的详细信息，请参见 Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，可用 Windows 资源管理器找到这个文件。在 Windows 95 及早期版本，或在 MS-DOS 中，可用 **Extract** 命令访问该文件。

可用 Setup Manager 完成以下任务，而后生成应答文件参数的结果。

- 指定应答文件的平台（Microsoft Windows 2000 Professional、Windows 2000 Server、远程操作系统安装或 Sysprep）。
- 指定无人参与安装模式的自动级别。级别包括“提供默认值”、“全部自动”、“隐藏页面”、“只读” 和“GUI 模式安装”。”
- 指定默认的用户信息。
- 定义计算机名称选项，包括创建唯一性数据库文件 (/UDF) 来访问带有效计算机名的文件。
- 配置网络设置。
- 创建分发文件夹。
- 添加自定义徽标和背景文件。

- 把文件添至分发文件夹。
- 把命令添至 [GuiRunOnce] 节。
- 创建 Cmdlines.txt 文件。
- 指定代码页。
- 指定区域选项。
- 指定时区。
- 指定 TAPI 信息。

Setup Manager 无法执行以下功能：

- 指定系统组件，如 Internet 信息服务。
- 创建 Txtsetup.oem 文件。
- 在分发文件夹中创建子文件夹。

表 25.3 介绍了由 Setup Manager 创建的一些最常见的应答文件规范。

表 25.3 Setup Manager 创建的应答文件规范

参数	目的
安装路径	在要安装 Windows 2000 Server 的目标计算机上指定需要的路径。
升级选项	指定是从 Windows 95、Windows 98、Windows NT 还是 Windows 2000 升级。
目标计算机名	指定应用于目标计算机的用户名、单位名称和计算机名称。
产品 ID	指定从产品文档中得到的产品标识号。
工作组或域	指定计算机所属的工作组或域的名称。
时区	指定计算机的时区。
网络配置信息	指定网卡类型和网络协议的配置。

手动创建应答文件

可用记事本之类的文本编辑器手动创建应答文件。一般情况下，应答文件由节标题、参数及这些参数的值组成。尽管大部分节的标题是事先定义的，您仍可定义其他节标题。请注意，如果安装不需要，就不必在应答文件中指定所有可能的参数。

无效参数值会在安装后产生错误或导致不正确的行为。

应答文件格式如下：

```
[section1]
;
; Section contains keys and the corresponding
; values for those keys/parameters.
; keys and values are separated by ' = ' signs
; Values that have spaces in them usually require double quotes
; "" around them
;
key = value
.
.
[section2]
key = value
```

.
.

使用应答文件设置密码

在安装中使用应答文件，让您可为以下密码命令设置参数：

- AdminPassword
- UserPassword
- DefaultPassword
- DomainAdminPassword
- AdminstratorPassword
- Password

有关这些命令定义的信息，请参见在 Windows 2000 操作系统 CD 上的“ Microsoft Windows 2000 Guide to Unattended Setup ”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，可用 Windows 资源管理器找到这个文件。在 Windows 95 及早期版本，或在 MS-DOS 中，可用 **Extract** 命令访问该文件。

另外，在本书附录“ 无人参与安装的应答文件示例 ”中，可以找到一些使用其中一些参数的应答文件示例。

备注　密码应限制在 127 个字母以内。如果指定的密码超过了 127 个字符，则会因为密码无效而无法登录系统。

安装完成后，虽然计算机中会保留一个应答文件，包含配置计算机所用的全部设置；但所有密码信息都会从应答文件本地复本中删除，这样就不会使安全受到破坏。

警告　但是，在安装程序过程中，应答文件是可在硬盘上使用的。因此，如果关心安全问题，请不要把密码信息添至为自动安装而创建的应答文件中。

使用本地应答文件使您可自动设置可选组件，方法是：运行那些包含已提供参数的命令（在与安装程序一起使用的原始应答文件中提供这些参数）。这些组件包括把服务器配置成域控制器、集群服务器或是启用消息队列。

扩展硬盘分区

您可以先在一个小分区（较大磁盘的 1 兆字节 [GB] 左右）上开始安装，然后使用应答文件中的 ExtendOEMPartition 参数，在 Windows 2000 安装过程中扩展这一分区。ExtendOEMPartition 参数只可在 NTFS 分区使用；它既可用于常规应答文件，也可用于基于 Sysprep 安装的应答文件。

关于 Sysprep 和 Sysprep.inf 文件的详细信息，请参见本章后面的“ 使用 Sysprep 复制磁盘 ”。

备注　ExtendOEMPartition 只在活动系统分区上起作用。在同一硬盘的其他分区，或计算机其他硬盘的其他分区上，都无法使用。此外，当使用 ExtendOemPartition=1 时，虽然它会扩展到硬盘上的所有剩余空间，但会把最后一个磁道留为空白。这是有意设计好的，以便您可以选择启用动态卷。

如果在文件分配表（FAT）分区上的自动安装过程中使用 ExtendOEMPartition，则需要在应答文件的 [Unattended] 节指定 FileSystem=ConvertNTFS，这样可以先把分区转换成 NTFS。有关将 ExtendOEMPartition 用于基于 Sysprep 安装的详细信息，请参见本章后面的“使用 Sysprep 复制磁盘”。

关于使用 ExtendOemPartition 的详细信息，请参阅在 Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，可用 Windows 资源管理器找到这个文件。在 Windows 95 及早期版本，或在 MS-DOS 中，可用 **Extract** 命令访问该文件。

检查 Windows 2000 安装命令

要安装 Windows 2000，必须运行恰当的 Windows 2000 安装程序：Winnt.exe 或 Winnt32.exe。在本章中，Winnt.exe 和 Winnt32.exe 均称为安装。以下因素决定了需要运行的安装类型。

- 要在运行 MS-DOS 或 Microsoft® Windows® 3.*x* 的计算机上执行全新安装，应在 MS-DOS 命令行运行 Winnt.exe。
- 要由 Windows NT、Windows 95 或 Windows 98 执行全新安装或升级，应运行 Winnt32.exe。

请注意，您可直接从启动软盘开始一个标准交互式安装，该启动软盘与 Windows 2000 Server CD 一起交付。

警告　如果您在升级为 Windows 2000 之前，更新了计算机上的应用程序，则一定要在运行安装程序之前重新启动计算机。

关于安装方法的详细信息，请参阅本章后面的“Windows 2000 Professional 自动安装”。

Winnt.exe

Winnt.exe 命令及其应用于自动安装的参数如下：

winnt [/S[:*sourcepath*]][/T[:*tempdrive*]]/U[:*answer_file*]][/R[x]:*folder*] [/E:*command*]

有关参数定义的详细信息，请参见本书附录“安装命令”。

对于有多个分区的硬盘驱动器，如果分区所含空间足够大，安装程序的 Winnt.exe 版本就会把 Windows 2000 安装在活动分区。否则，安装程序会搜寻包含足够空间的其他分区，并提示您选择想要的分区。如果是自动安装，则可运行带 **/T** 参数的安装程序，这样可跳过提示，自动指向想要的分区。例如：

winnt [/unattend] [:<path>\answer.txt] [/T[:d]]

Winnt32.exe

Winnt.exe 命令及其应用于自动安装的参数如下：

winnt32 [/s:*sourcepath*] [/tempdrive:*drive_letter*]
[/unattend[*num*][:*answer_file*]] [/copydir:*folder_name*]
[/copysource:*folder_name*] [/cmd:*command_line*]
[/debug[*level*][:*filename*]]
[/udf:*id*[,*UDB_file*]] [/syspart:*drive_letter*] [/noreboot]
[/makelocalsource] [/checkupgradeonly] [/m:*folder_name*]

有关参数定义的详细信息，请参见本书附录“安装命令”。

对于有多个分区的硬盘驱动器，如果分区包含足够空间的话，安装程序的 Winnt32.exe 版会把 Windows 2000 安装在活动分区上。否则，安装程序会搜寻包含足够空间的其他分区，并提示您选择想要的分区。如果是自动安装，则可运行带 /tempdrive 参数的安装程序，这样即可绕过提示，自动指向想要的分区。例如：

```
winnt32 [/unattend] [:<path>\answer.txt] [/tempdrive:d]
```

为了安装到目标计算机，Windows 2000 最多可用八个 **/S** 开关指向作为源位置的其他分布服务器。此功能可以加快安装程序向目标计算机复制文件的阶段，同时还可为运行安装程序的分发服务器提供额外的负载平衡能力。例如：

```
<path to distribution folder 1>\winnt32 [/unattend]
[:<path>\answer.txt] [/s:<path to distribution folder 2>] [/s:<path
to distribution folder 3>] [/s:<path to distribution folder 4]
```

表 25.4 显示了安装命令及其如何与 Windows 2000 一起使用。

表 25.4 使用安装命令

安装命令	Windows 2000 版本	升级	全新安装
Winnt.exe	Server 和 Professional	否	是
Winnt32.exe	Server 和 Professional	是	是

客户应用程序的自动安装

解决了关键规划问题后，就可以决定如何执行服务器应用程序自动安装了。几乎所有情况下，您都会想用应用程序的无人参与安装功能来完成安装。

可从如下三种方式中选择：

- Cmdlines.txt
- 由应答文件的 [GuiRunOnce] 节运行应用程序安装程序或者批处理文件。
- Windows 安装服务

使用 Cmdlines.txt

Cmdlines.txt 文件包含了一些命令，GUI 模式在安装可选组件（比如安装 Windows 2000 Professional 之后必须立即安装的应用程序）时会执行这些命令。如果打算使用 Cmdlines.txt，则需把它放入分发文件夹的 OEM 子文件夹中。如果使用 Sysprep，则应把 Cmdlines.txt 放入 OEM\$1\Sysprep 子文件夹中。

当存在以下条件时，请使用 Cmdlines.txt：

- 正由分发文件夹的 OEM 子文件夹进行安装。
- 正在安装的应用程序具有以下属性：

  它不会为多个用户自动配置（例如， Microsoft® Office 95 ）。

  – 或 –

  设计成由一个用户安装并复制用户特定信息。

Cmdlines.txt 的语法如下所示：

```
[Commands]
"<command_1>"
"<command_2>"
.
.
"<command_x>"
```

参数定义如下：

- *"<command_1>"*、*"<command_2>"*、一直到 *"<command_x>"* 指 GUI 模式调用 Cmdlines.txt 时要运行的命令（及以何种顺序）。注意所有的命令必须在引号中。

使用 Cmdlines.txt 时，要注意以下情况：

- 当 Cmdlines.txt 中的命令在安装过程中执行时，不存在已登录的用户和可以保证的网络连接。因此，用户特定信息会写入默认的用户注册表，并且所有以后创建的用户都会收到该信息。
- Cmdlines.txt 要求将运行应用程序或工具所需的文件放在安装过程会访问的目录中，也就是这些文件必须在硬盘上。

使用应答文件的 [GuiRunOnce] 节

应答文件的 [GuiRunOnce] 节包含了安装程序运行后用户首次登录到计算机时运行的命令列表。例如，可在 [GuiRunOnce] 节输入以下内容，以开始自动执行应用程序安装程序：

```
[GuiRunOnce]
"%systemdrive%\appfolder\appinstall -quiet"
```

如果要用 [GuiRunOnce] 启动安装程序，则需考虑一些其他因素：

如果应用程序强行重新启动，请确定是否有方法禁止重新启动 这很重要，因为每次系统重新启动，[GuiRunOnce] 节中所有以前的条目都会丢失。如果尚未完成以前列在 [GuiRunOnce] 节的项目时就重新启动了系统，剩余项目将不会运行。如果应用程序本身无法禁止重新启动，可试着把应用程序重新打包成“ Windows 安装服务 ”软件包。一些第三方产品可提供这一功能。

Windows 2000 包括 WinINSTALL Limited Edition (LE)，它是 Windows 安装服务用来重新打包的工具。您可用 WinINSTALL LE 有效地重新打包 Windows 安装服务之前的应用程序，使其成为能够用 Windows 安装服务分发的软件包。关于 WinINSTALL LE 的详细信息，请参阅 Windows 2000 操作系统 CD 上的 \Valueadd\3rdparty\Mgmt\Winstle 文件夹。

有关 Windows 安装服务打包的详细信息，请参见本章后面的“ 使用 Windows 安装服务 ”。

重要提示 如果正把应用程序安装到 Windows 2000 的多个本地语言版本，则建议您在本地化版本上测试重新打包的应用程序，以确保应用程序把文件复制到了正确的位置并恰当地写入了注册表项目。

如果应用程序需要安装 Windows 资源管理器外壳，则会因为 Run 和 RunOnce 命令时执行时未载入该外壳，导致 [GuiRunOnce] 节不会奏效。请与应用程序供应商核实，确定是否有升级版本或补丁程序可解决应用程序安装的这种情况。如果没有，可以将应用程序重新打包成 Windows 安装服务软件包或使用其他的分发方法。

相同安装机制类型的应用程序如果不使用 /wait 命令也可能不会正常运行。在应用程序安装正在运行时如果又启动了另一进程，则有可能会发生这种情况。安装程序例程还在运行时，如果初始化其他进程或关闭当前的活动程序，可能会导致 RunOnce 项目列表中的下一个例程启动。由于有一个以上的安装机制实例正在运行，第二个应用程序通常会失败。有关如何使用批处理文件控制这一问题的详细信息，请参见本章后面的“ 使用批处理文件控制多个应用程序的安装 ”。

使用应用程序安装程序

预装应用程序的首选方法是使用与应用程序一起提供的安装例程。如果要预装的应用程序可以在安静模式（即没有用户干预）下使用 **/q** 或 **/s** 命令行开关运行，就可以这样做。有关安装机制支持的命令行参数的列表，请参阅该应用程序的帮助文件或文档。

以下是一个命令行的示例，您可以将其放进 [GuiRunOnce] 节，以用应用程序本身的安装程序初始化无人参与安装。

<path to setup>\Setup.exe /q

安装程序参数会因应用程序的不同而不同。例如，想要创建监视安装的日志文件时，有些应用程序所含的 **/l** 参数会很有用。一些应用程序有防止自动重启的命令。这些命令将有助于控制应用程序的安装，尽量减少重启次数。

预装任何应用程序之前，一定要与应用程序供应商核实信息、使用说明、工具以及最佳做法的信息。

重要提示 对任何应用程序，无论如何安装，都必须满足其许可要求。

使用批处理文件控制多个应用程序的安装

要控制多个应用程序的安装，可以创建包含独立安装命令的批处理文件并使用带有 **/wait** 命令行开关的 **Start** 命令。这种方法可以保证应用程序按顺序安装，每个应用程序在下一应用程序开始其安装程序例程之前就已经全部安装完毕。批处理文件会从 [GuiRunOnce] 节开始运行。

以下步骤说明了如何创建批处理文件、如何安装应用程序以及应用程序安装完毕后如何删除所有对批处理文件的引用。

要使用批处理文件安装应用程序：

1. 创建包含类似下行示例的批处理文件：

   Start /wait <path to 1st application>\Setup <command line parameters>
   Start /wait <path to 2nd application>\Setup <command line parameters>
   Exit

   此处：

   - *<path>* 是启动安装程序的可执行文件的路径。该路径在安装过程必须可用。
   - *Setup* 是启动安装程序的可执行文件的名称。
   - *<command line parameters>* 是可用的安静模式参数，适用于要安装的应用程序。

2. 把批处理文件复制到分发文件夹上或者其他安装过程中可以访问的位置。

3. 以 *<filename>*.bat 作为批处理文件名，在应答文件 [GuiRunOnce] 节中加入一项来运行批处理文件，如下例所示。本示例假设批处理文件已经复制到本地硬盘的 Sysprep 文件夹上，尽管它可以放置在安装过程中安装程序可以访问的任何位置。

   [GuiRunOnce]
   "%systemdrive%\sysprep*<filename>*.bat"= "*<path-1>**Command-1.exe*"
   "*<path-n>*|*Command-n.exe*"
   "%systemdrive%\sysprep\sysprep.exe –quiet"

此处：

<path-1>|Command-1.exe 和 *<path-n>|Command-n.exe* 是到其他应用程序、工具安装程序或配置工具的完全合格的路径。也可以是其他批处理文件的路径。这些路径在安装过程必须可用。

使用 Windows 安装服务

Windows 安装服务是使多个计算机上的应用程序安装标准化的 Windows 2000 组件。

如果不使用 Windows 安装服务来安装应用程序，每个应用程序就必须有其自己的可执行安装程序文件或脚本。每个应用程序必须确保遵循正确的安装规则（比如，创建文件版本的规则）。这是因为，应用程序安装并非操作系统开发不可分割的一部分，所以也就没有关于安装规则的权威参考。

Windows 安装服务可实施操作系统本身所有正确的安装规则。要遵循这些规则，必须用称为 Windows 安装服务软件包的标准格式来描述应用程序。包含格式信息的数据文件称为 Windows 安装服务包文件并有 .msi 的扩展名。Windows 安装服务使用 Windows 安装服务包文件安装应用程序。

Windows 安装服务术语

下列术语描述使用 Windows 安装服务技术的安装过程：

资源。一般情况下安装服务发送给计算机的文件、注册表项目、快捷方式或其他元素。

组件。可作为一个单元进行安装或卸载的文件、注册表项目及其他资源的集合。当安装或删除某个选中的组件时，该组件中的所有资源也会同时安装或删除。

功能。用户可以选择安装的应用程序的细化部分。功能通常代表应用程序本身的功能特性。

产品。单一的产品，例如 Microsoft® Office。产品包括一个或更多的功能。

Windows 安装服务软件包文件

软件包文件是一种用于安装性能的优化的数据库格式。通常，这个文件描述了特定产品的功能、组件及资源之间的关系。

Windows 安装服务软件包文件通常都和产品文件一起放在产品 CD 或网络映射的根文件夹上。产品文件以称为箱盒文件（带 .cab 扩展名）的压缩文件形式存在。每一个产品都有它自己的软件包文件。在安装时，Windows 安装服务会打开当前产品的软件包文件，并用 Windows 安装服务软件包中的信息确定必须为该产品执行的所有安装操作。

Windows 2000 Professional 的自动安装

在企业环境中，如果在每台计算机上都进行标准的交互式 Windows 2000 安装，其性能价格比不够理想。为了大幅降低总体拥有成本 (TCO)，可以在多个计算机上执行 Windows 2000 Professional 自动安装。

您可以进行以下类型的自动安装：

- Windows 2000 Professional 的核心操作系统。

- 标准的生产效率应用程序，例如 Microsoft® Office 2000 或其他任何不作为服务运行的程序。
- 通过安装不同语言包，实现对 Windows 2000 Professional 的额外语言支持。
- Windows 2000 Professional 的 service pack。

Windows 2000 Professional 的自动安装包括运行带有应答文件的安装程序。安装可以以无人参与的方式运行。无人参与安装包括如下步骤：

- 创建应答文件。
- 确定并实施一个过程来配置特定的计算机信息。
- 使用 Windows 安装服务软件包，为安装其他文件做准备。
- 确定并执行该进程，以自动执行选定的分布方法，例如使用网络分布点或硬盘复制。

自动安装的新选项

Windows 2000 自动安装中，应答文件有几个用来控制运行方法及运行内容的新选项。有关应答文件参数和语法的详细信息，请参见 Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，可用 Windows 资源管理器找到这个文件。在 Windows 95 及早期版本，或在 MS-DOS 中，可用 **Extract** 命令访问该文件。

柔性网络 Windows 2000 中，每台计算机都有可用的灵活网络配置，包括对协议、服务和客户的附加支持。现在可以设置绑定顺序，这样就可方便地设置默认信息，及在系统中安装不止一个网卡。另外，为使安装和配置更容易，Windows 2000 可以自动安装和配置网络设备驱动程序。默认情况下，除非应答文件中另有规定，否则 Windows 2000 会在系统的每个网卡上都安装默认的网络组件。默认网络组件包括 Microsoft 网络客户、TCP/IP、Microsoft 网络文件和打印共享，及启用动态主机配置协议 (DHCP)。

自动登录能力 可以自定义应答文件，使计算机能在安装完毕后首次启动 Windows 2000 时，或在特定的启动次数后，自动以管理员的身份登录。如需要 Windows 2000 自动按指定的次数登录，以完成 RunOnce 项目中运行的任务，则需要在应答文件中提供一个非空的管理员密码 (AdminPassword)。 然后即可用 AutoAdminLogonCount，指定要完成期望的任务而需要系统自动登录的次数。如果使用了空密码，安装程序将只能有一次是自动登录系统，而无法通过其他方法为以后的每次重新启动提供凭据。这样做是为了降低安全风险。请注意，如果在文本文件中提供了管理员帐户凭信，而又有用户可以访问该文件，则会产生安全风险。

自动命令执行 应答文件的 [GuiRunOnce] 节包含要在 GUI 模式完成后作为安装程序一部分连续执行的命令列表。使用 [GuiRunOnce]，可以指定要安装的应用程序、配置系统的工具或用户首次登录到已安装的计算机时要运行的工具的列表。

简化的时区规范 在应答文件中，指定计算机时区变得更加容易，而且，与 Windows NT 相比所需的调试更少。因为列举了所有可能的时区，而不必输入完整的时区字符串，从而减少了出错的机会。

增强的区域和语言设置 在应答文件中，您可以指定系统和用户位置、键盘和输入方法以及要安装的语言支持。当您使用向导的 GUI 界面来选择要安装在系统上的设置时，Setup Manager 就可以简化以上操作。

简化的设备预装 由于引入了即插即用、OemPnPDriversPath 关键字、新的分发共享点结构，所以预装设备变得更为简单，只需把新驱动程序添至分发共享点的一个文件夹并指定 OemPnPDriversPath 关键字即可。

自动安装方法

可以用几种方法运行 Windows 2000 Professional 自动安装。正如本章上文所述，选择的方法取决于关键规划的结果。

在客户计算机上进行自动安装的方法包括：

- 在有不同硬件的计算机上使用 Syspart。
- 使用 Sysprep 复制磁盘。
- 使用 Systems Management Server
- 使用引导 CD-ROM。
- 使用远程操作系统安装程序

  备注 远程操作系统安装程序可自动从指定的远程安装服务（RIS）服务器上把 Windows 2000 Professional 和应用程序安装到客户计算机上。RIS 是 Windows 2000 Server 包括的一个可选组件。

表 25.5 描述了每种自动安装方法的使用时机。

表 25.5 何时使用自动安装方法

方法	用途
Syspart	用于拥有不同硬件计算机的全新安装。
Sysprep	主控计算机和目标计算机有相同硬件（包括 HAL 和大型存储设备控制器）时使用。
SMS	用于对多个系统执行 Windows 2000 Server 的管理升级，特别是在这些系统地点分散时。
引导 CD-ROM	在基本输入/输出系统（BIOS）允许用引导 CD-ROM 启动的计算机上使用。
远程操作系统安装	用于在所支持的计算机上远程安装 Windows 2000 Professional 的映像，从而避免了物理访问每台计算机来执行安装。

在有不同硬件的计算机上使用 Syspart

Syspart 通过 Winnt32.exe 的一个可选参数运行。如果主控计算机和要安装 Windows 2000 Professional 的计算机没有相似的硬件，就可以使用 Syspart 方法。 这种方法还通过免去了安装的文件复制阶段，减少了部署时间。

Syspart 要求使用两个物理磁盘，而且在目标硬盘上有主分区。

如果要在 HAL 或大型存储设备控制器不同的硬件类型上进行相似的安装和操作系统配置，可先用 Syspart 创建一组主控文件，这些文件有必需的配置信息及可映射的驱动程序支持。然后这些映像就可用在不同的系统中，对硬件进行适当的检测，并一致地配置基本操作系统。如果环境包含多种“硬件-依赖”型的系统，您可以使用 Syspart 为每种类型分别创建主控。可先在每种类型的一台计算机上安装 Windows 2000，然后用 Sysprep 创建映射，用于各类型其余的计算机。有关 Sysprep 的详细信息，请参见本章后面的“使用 Sysprep 复制磁盘”。

在开始之前，要选择一台作为参照的计算机。参照计算机必须安装了 Windows NT 或 Windows 2000。

要用 Syspart 安装 Windows 2000 Professional

1. 先启动参照计算机并连接到安装分发文件夹。
2. 运行安装程序。

   单击“开始”，再单击“运行”，然后键入：

   winnt32 /unattend:unattend.txt /s:*install_source*
   /syspart:*second_drive* /tempdrive:*second_drive/* noreboot

   重要提示 为了成功完成 Syspart 安装，必须使用 */tempdrive* 参数。当使用 **/***tempdrive* 命令行开关时，要保证在第二分区上有足够的可用磁盘空间，以用来安装 Windows 2000 Server 和应用程序。作为 Syspart 目标的磁盘几何结构必须与要复制的计算机的磁盘几何结构相同。

   注意 */syspart* 和 */tempdrive* 参数必须指向副硬盘的同一分区。Windows 2000 Professional 的安装必须在副硬盘的主分区上进行。

   警告 Syspart 会自动把驱动器标记为活动的和默认的启动设备。因此，再次启动计算机之前，应删除该驱动器。

   相关的定义包括：

   Unattend.txt。用于无人参与安装的应答文件。在安装过程中，用户通常会对提示做出响应，该文件为这些提示的一部分或全部提供了答案。创建主映像时，可选择是否使用应答文件。

   install_source。Windows 2000 Professional 文件的位置。如果想同时从多个源进行安装，应指定多个 **/s** 命令行开关。

   second_drive。一个预装了 Windows 2000 和应用程序的可选的副驱动器。

使用 Sysprep 复制磁盘

如果要在多台计算机上安装相同的配置，磁盘复制是一个很好的选择。先在主控计算机上，安装 Windows 2000 和任何要安装在所有目标计算机上的应用程序。然后运行 Sysprep 把该映像传送给其他计算机。为了向其他计算机的复制，Sysprep 会在主控计算机上准备硬盘，随后运行一个第三方磁盘映射进程。与标准安装或脚本安装相比，这种方法大大地减少了部署时间。

要使用 Sysprep，主控计算机和目标计算机必须有相同的 HAL、高级配置和电源接口 (ACPI) 支持以及大型存储设备控制器。当计算机在运行 Sysprep 后启动时，Windows 2000 会自动检测即插即用设备，Sysprep 将重新检测并列出系统设备。这就是说，主控计算机和目标计算机上的即插即用设备，如网卡、调制解调器、视频适配器和声卡可以不必相同。Sysprep 安装的主要优势在于速度。映像可以打包和压缩，并且只有特定配置所需的文件才会作为映像的一部分而创建。同时，还会创建在其他系统上可能需要的其他即插即用驱动程序。映像也可以复制到 CD 上，然后分发到链接速度缓慢的远程站点。

备注 由于要求主控和目标计算机有相同的 HAL、ACPI 支持以及大型存储设备，所以可能需要您为环境保留多个映像。

重要提示 执行磁盘复制时，请与软件供应商核实，确认不会违反待复制软件的安装许可协议。

Sysprep 过程概述

本节描述了建立用于磁盘复制的源计算机的过程。

1. 安装 Windows 2000——在与想要的目标计算机有相似硬件的计算机上安装 Windows 2000 Professional。建立计算机时，不能将其加入域，并且必须把本地管理密码留为空白。

2. 配置计算机——作为管理员登录，然后安装并自定义 Windows 2000 Professional 和相关的应用程序。这有可能包括提高工作效率的应用程序，如 Microsoft® Office 2000、专用的商业应用程序；以及要包括在所有客户的常用配置中的应用程序或设置。

3. 验证映像——按您定义的准则运行审核，以验证映像配置是否正确删除残留信息，包括审核和事件日志遗留的所有信息。

4. 准备要复制的映像——当确信计算机已完全按照所需方式配置以后，就可以准备复制系统了。可用可选文件 Sysprep.inf 运行 Sysprep 来完成这一步，这一点在本章后面进行说明。Sysprep 完成后，计算机自动关机或显示可以安全关机。

5. 复制——此时计算机硬盘起动并运行即插即用检测，创建新的安全识别器 (SID)，然后在下次启动系统时运行小型安装程序向导。现在已准备好使用硬件或软件解决方案复制或映射系统。下一次 Windows 2000 从这个硬盘上或从任何在该映像上创建的复制硬盘上启动时，系统会检测和重新列出即插即用设备，以完成目标计算机的安装和配置。

   重要提示 依赖 Active Directory 的组件不能被复制。

Sysprep 文件

要使用 Sysprep，可手动运行 Sysprep.exe，也可通过使用应答文件的 [GuiRunOnce] 节配置安装程序自动运行 Sysprep.exe。为了运行 Sysprep，Sysprep.exe 和 Setupcl.exe 文件必须位于系统驱动器 (%systemdrive%\Sysprep\) 根目录下的 Sysprep 文件夹中。要在自动安装过程中，把文件放置在正确的位置，必须把这些文件添至 OEM\$1\Sysprep 子文件夹下的分发文件夹中。有关该子文件夹的详细信息，请参见本章前面的“构建分发文件夹”。

这些文件为复制操作系统作准备并启动小型安装程序向导。您也可以在 Sysprep 文件夹中包括一个可选的应答文件 Sysprep.inf。Sysprep.inf 包含了可用来在合适位置提供一致响应的默认参数。这可以限制对用户输入的要求，从而减少了可能会发生的用户错误。也可以把 Sysprep.inf 文件放置在软盘上，当 Windows 启动屏幕出现后，将软盘放进软盘驱动器，就可以在目标计算机上进行进一步的自定义。当“请稍候”小型安装程序向导屏幕出现时，软盘驱动器开始读取。小型安装程序向导成功完成其任务时，系统会最后一次重新启动，Sysprep 文件夹及其所有内容被删除，系统为用户登录作好准备。

以下节定义了 Sysprep 文件。

Sysprep.exe

Sysprep.exe 有下列的三个可选参数：

quiet — 运行 Sysprep 时不显示屏幕消息。

nosidgen — 运行 Sysprep 时不再生成系统已有的 SID。如果不打算复制运行 Sysprep 的计算机，使用该参数会很有效。

reboot – Sysprep 关闭计算机后自动重新启动。这样就不必再手动启动计算机了。

Sysprep.inf

Sysprep.inf 是用来使小型安装程序过程自动化的应答文件。它使用与安装程序应答文件相同的 .ini 文件语法和关键字名称（为所支持的关键字）。需要把 Sysprep.inf 文件放在 %systemdrive%\Sysprep 文件夹中或软盘上。如果使用软盘，可以在 Windows 启动屏幕出现以后提供软盘。请注意，如果运行 Sysprep 时并未包括 Sysprep.inf，小型安装程序向导就会显示本章下文“小型安装程序向导”列出的所有可用的对话框。

备注 如果在主控计算机上提供了 Sysprep.inf 文件，而且要根据每台计算机更改 Sysprep.inf，就可使用上文讨论过的软盘方法。

以下是 Sysprep.inf 文件的一个示例：

```
[Unattended]
;Prompt the user to accept the EULA.
OemSkipEula=No
;Use Sysprep's default and regenerate the page file for the system
;to accommodate potential differences in available RAM.
KeepPageFile=0
;Provide the location for additional language support files that
;may be needed in a global organization.
InstallFilesPath=%systemdrive%\Sysprep\i386

[GuiUnattended]
;Specify a non-null administrator password.
;Any password supplied here will only take effect if the original
source
;for the image (master computer) specified a non-null password.
;Otherwise, the password used on the master computer will be
;the password used on this computer.This can only be changed by
;logging on as Local Administrator and manually changing the password.
AdminPassword=""
;Set the time zone
TimeZone=20
;Skip the Welcome screen when the system boots
OemSkipWelcome=1
;Do not skip the regional options dialog so that the user can
indicate
;which regional options apply to them.
OemSkipRegional=0

[UserData]
;Prepopulate user information for the system
FullName="Authorized User"
OrgName="Organization Name"
ComputerName=XYZ_Computer1

[Identification]
;Join the computer to the domain ITDOMAIN
JoinDomain=ITDOMAIN

[Networking]
;Bind the default protocols and services to the (s) network card used
;in this computer.
InstallDefaultComponents=Yes
```

备注 只有现有的管理密码为空时，才能用 Sysprep.inf 更改管理密码。要用 Sysprep GUI 更改管理员密码时也是如此。

有关应答文件参数和语法的详细信息，请参见 Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，可用 Windows 资源管理器找到这个文件。在 Windows 95 及早期版本，或从 MS-DOS 中，可用 **Extract** 命令访问该文件。

Setupcl.exe

Setupcl.exe 完成以下任务：

- 为计算机重新生成新的 SID。
- 启动小型安装程序向导。

小型安装程序向导

当计算机通过 Sysprep 方法复制的磁盘启动时，小型安装程序向导将首次启动。该向导会收集进一步自定义目标计算机所需的任何信息。如果不使用 Sysprep.inf，或把该文件的某些节留为空白，小型安装程序向导就会显示那些 Sysprep.inf 未提供应答的屏幕。可能的屏幕包括：

- 最终用户许可协议（EULA）
- 区域选项
- 用户名和公司
- 计算机名和管理员密码
- 网络设置
- TAPI 设置（仅在计算机有调制解调器或新的调制解调器设备时显示）
- 服务器授权（只对服务器）
- 时区选择
- 完成/重新启动

要想跳过这些屏幕，可以在 Sysprep.inf 内指定某些参数。表 25.6 中列出了这些参数。

备注 由于安装程序会检测显示设备的最佳设置，所以当安装程序或者小型安装程序向导运行时看不到“显示设置”屏幕。可以在主控计算机所用的应答文件或目标计算机所用的 Sysprep.inf 文件的 [Display] 节指定这些设置。如果 [Display] 节的设置是在主控计算机所用的应答文件中，那么，除非 Sysprep.inf 包括不同设置，或者检测到的视频适配器或监视器需要与主控计算机不同的设置，否则 Sysprep 就会保留这些设置。

表 25.6 跳过小型安装程序向导所需的 Sysprep.inf 参数

参数	值
区域选项	[RegionalSettings] section [GuiUnattended] OemSkipRegional=1
用户名和公司	[UserData] FullName="User Name" OrgName="Organization Name"
计算机名和管理员密码	[UserData] ComputerName=W2B32054 [GuiUnattended] AdminPassword=""
TAPI 设置	[TapiLocation] AreaCode=425
网络设置	[Networking] InstallDefaultComponents=Yes

服务器授权（只对服务器）	[LicenseFilePrintData] AutoMode = PerServer AutoUsers = 5
时区选择	[GuiUnattended] TimeZone=<desired time zone index>
完成/重新启动	N/A

手动运行 Sysprep

安装 Windows 2000 Professional 之后，可使用 Sysprep 准备把系统传送到拥有类似配置的计算机上。要手动运行 Sysprep，必须先安装 Windows 2000 Professional，配置系统并安装应用程序。然后运行不带 *–reboot* 命令行开关的 Sysprep。系统关闭后，把驱动器映像复制到有类似配置的计算机上。

当用户首次启动复制的计算机时，Sysprep 小型安装程序将会运行，使用户能够自定义其系统。也可用 Sysprep.inf 预先指定 Sysprep 的部分或全部配置参数。Sysprep 小型安装程序完成后，Sysprep 文件夹（包括 Sysprep.exe 和 Setupcl.exe）会被自动删除。

要为复制 Windows 2000 Professiona 的安装做准备：

1. 在“开始”菜单上，单击“运行”，然后键入：

   cmd

2. 在命令提示符下，转换成 C 驱动器的根文件夹，然后键入：

   md sysprep

3. 把 Windows 2000 Professional CD 放入恰当的驱动器。打开 \Support\Tools 文件夹中的 Deploy.cab 文件。

4. 将 Sysprep.exe 和 Setupcl.exe 复制到 Sysprep 文件夹中。

   如果正在使用 Sysprep.inf，也把该文件复制到 Sysprep 文件夹。请注意，Sysprep.exe、Setupcl.exe 和 Sysprep.inf 必须在同一个文件夹中，这样 Sysprep 才可正常运行。

5. 在命令提示符下，要转换到 Sysprep 文件夹，键入如下内容：

   cd sysprep

6. 根据需要，键入以下内容：

   Sysprep
   Sysprep –reboot
   Sysprep */<optional parameter>*
   Sysprep */<optional parameter>* -reboot
   Sysprep */<optional parameter 1>*U/*<optional parameter X>*
   Sysprep */<optional parameter 1>*U/*<optional parameter X>* -reboot

7. 如果没有指定 *–reboot* 命令行开关，请执行以下操作：

   当出现信息，提示您关闭计算机时，在“开始”菜单处单击“关闭系统”。现在准备用第三方磁盘映射工具创建安装的映像。

   如果指定 *–reboot* 命令行开关只用于审核目的，计算机就会重新启动并运行小型安装程序向导。执行下列任务：

- 验证小型安装向导是否提供了所需的提示。还可同时审核系统和其他应用程序。完成审核后，再次运行不带 *–reboot* 命令行开关的 Sysprep。
- 当出现信息，提示您关闭计算机时，在“开始”菜单处单击“关闭系统”。现在准备用第三方磁盘映射工具创建安装的映像。

备注 要使安装程序处理 Cmdlines.txt 文件，可将其添至 Sysprep 文件夹。该文件用来运行安装程序以后的命令，包括安装应用程序所需的命令。

安装结束后自动运行 Sysprep

应答文件的 [GuiRunOnce] 节包含了要在安装程序结束后执行的一些命令。可用 [GuiRunOnce] 节创建安装，用于完成安装程序、自动登录到计算机、以 *–quiet* 模式运行 Sysprep，然后关闭计算机。要达到此目的，需要执行以下操作：

1. 要把文件复制到系统驱动器的正确位置，应把所需的 Sysprep 文件加入 OEM\$1\Sysprep\ 下的分发文件夹。
2. 在应答文件的 [GuiRunOnce] 节，建立计算机上最后运行的命令；命令如下：

   ```
   %systemdrive%\Sysprep\Sysprep.exe –quiet
   ```

   如果需要多次重新启动，应使其成为 [GuiRunOnce] 节最后一次使用时最后用到的命令。

使用 Sysprep 扩展磁盘分区

Windows 2000 GUI 安装程序和小型安装程序可通过应答文件扩展 NTFS 分区。这一新的功能会完成以下任务：

- 允许您创建可扩展到更大磁盘分区的映像，这样就可充分利用可能比主控计算机原始硬盘更大的硬盘。
- 提供一种在较小硬盘上创建映像的方法。

要确定把该功能并入环境的最好方法，需检查以下步骤，并根据映射操作系统的工具选择一种最佳方法。

警告 如果可用映射工具编辑映像，就能够删除 Pagefile.sys、Setupapi.log 和 Hyberfil.sys（如果有）文件，因为目标计算机运行小型安装程序向导时会重建这些文件。但一定不要在活动系统上删除这些文件，因为这会导致系统无法正常运行。即使需要也只能从映像上删除这些文件。

在使用第三方映射产品或支持 Windows 2000 所用的 NTFS 的硬件映射设备时扩展硬盘分区：

1. 配置主控计算机上的硬盘分区，使其满足安装 Windows 2000（含所有组件）及要预装的应用程序所需的最小空间。这会降低总的映像空间需求。
2. 在用于创建主控映像的应答文件的 [Unattended] 节中包括 FileSystem=ConvertNTFS。由于想保留最小的可能映像空间，就不必在此包括 ExtendOemPartition。

   备注 ConvertNTFS 在 Sysprep.inf 中无效，因为它是只用于文本模式的功能，而 Sysprep 无法进入文本模式。
3. 在 Sysprep.inf 的 [Unattended] 节加入如下语句：

   ```
   ExtendOemPartition = 1
   ```

(或以兆字节表示扩展分区的其他空间)

4. 在主控计算机上安装 Windows 2000。Sysprep 将自动关闭系统。
5. 映射驱动器。
6. 把映像放在目标计算机中，目标计算机的系统分区与主控计算机的大小相同。
7. 重新启动目标计算机。

   小型安装程序向导启动并几乎立即扩展分区。

在使用不支持 Windows 2000 所用的 NTFS 的映射产品时扩展硬盘分区

1. 配置主控计算机上的硬盘分区，使其满足安装 Windows 2000（含所有组件）及要预装的应用程序所需的最小空间。这会降低总的映像空间需求。
2. 用 Windows 2000 提供的 Convert.exe 工具把文件系统转换成 NTFS。
3. 把以下项目加入应答文件，作为其 [GuiRunOnce] 节的最后两项（该应答文件用于创建主控映像）：

   ```
   [GuiRunOnce]
   Command1 = "command line"
   Command2 = "command line"
   ...
   Commandn-1 = "Convert c:\ /fs:ntfs"
   Commandn = "%systemdrive%\sysprep\sysprep.exe - quiet"
   ```

   这里：

   - <command line> 包括安装应用程序或在映射操作系统前进行配置时需要运行的所有命令。
   - <Commandn-1> 是在应答文件的 [GuiRunOnce] 节执行的倒数第二个命令。
   - 这会运行“ Convert ”命令。由于 Convert 命令无法在操作系统运行时把活动系统转换成 NTFS，所以将在下次计算机重新启动时进行转换。因为 Sysprep 是下一个要运行的项目，所以在此过程中系统不会转换成 NTFS。
   - <Commandn> 是计算机运行的最后一个命令。该命令是 Sysprep.exe。Sysprep 运行时，它会先为计算机准备映射，然后关闭计算机。

   备注 在这一步中，不能把 ExtendOemPartition 加入主应答文件，因为映像生成的分区不是 NTFS。而且您可能想保留尽可能小的映像。

4. 在 Sysprep.inf 的 [Unattended] 节加入如下语句：

   ```
   ExtendOemPartition = 1
   ```

   (或以兆字节表示扩展分区的其他空间)

5. 在主控计算机上安装 Windows 2000。Sysprep 将自动关闭系统。

   重要提示 不要重新启动计算机。

6. 映射驱动器。
7. 把映像放在目标计算机中，目标计算机的系统分区与主控计算机的大小相同。
8. 重新启动目标计算机。

一开始计算机将以转换模式启动，以把目标计算机的系统分区转换成 NTFS。

计算机将自动重新启动。

小型安装向导启动，且几乎立即扩展分区。

使用 Systems Management Server

可用 SMS 执行多个系统中 Windows 2000 Professional 的管理升级，特别是在这些系统地点分散时。请注意，只有计算机有以前安装的操作系统时，才可以用 SMS 进行安装。使用 SMS 升级之前，要先评估现有的网络基本配置，包括带宽、硬件和地区限制。使用 SMS 升级的主要好处在于您可以对升级过程保持集中控制。例如，您可以控制何时升级（例如，在培训过程中或之后、硬件验证之后和用户数据备份之后），控制哪些计算机需要升级，以及如何应用网络约束。有关 SMS 部署的详细信息，请参见本书中的“使用 Systems Management Server 部署 Windows 2000”。

使用引导光盘

对于其基本输入/输出系统（BIOS）允许通过 CD 启动的计算机，您可用引导 CD 方法安装 Windows 2000 Professional。这种方法对链接较慢、没有本地 IT 部门的远程站点上的计算机非常有用。引导 CD 方法将运行 Winnt32.exe，该文件允许进行快速安装。

备注 只能把引导 CD 方法用于全新安装。要进行升级，则必须在现有的操作系统中运行 Winnt32.exe。

为了保证最大程度的灵活性，请把 BIOS 的启动顺序设置如下：

- 网卡
- CD
- 硬盘
- 软盘

要使用引导 CD，必须满足以下条件：

- 计算机必须有对引导的 CD 的 El Torito No Emulation 支持。
- 应答文件必须包含带必需关键字的 [Data] 节。
- 应答文件必须命名为 Winnt.sif 并位于软盘上。

有关应答文件参数和语法的详细信息，请参见 Windows 2000 操作系统 CD 上的“Microsoft Windows 2000 Guide to Unattended Setup”(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，可用 Windows 资源管理器找到这个文件。在 Windows 95 及早期版本，或从 MS-DOS 中，可用 **Extract** 命令访问该文件。

要使用引导 CD 安装 Windows 2000

1. 通过 Windows 2000 CD 启动系统。
2. 当“Windows 2000 安装程序”的蓝色文本模式屏幕出现时，把有 Winnt.sif 文件的软盘放入软盘驱动器中。

3. 计算机读取软盘驱动器后，取出软盘。安装程序将按 Winnt.sif 文件的规定从 CD 运行。

   备注 引导 CD-ROM 方法要求所有必须的文件都在 CD-ROM 上。唯一性数据库文件 (UDF) 不能应用于这种方法。

使用远程操作系统安装程序

远程操作系统安装程序是 Windows 2000 Server 所含的一个可选组件，它以远程安装服务 (RIS) 技术为基础。因为 RIS 使用基于前引导执行环境 (PXE) 的远程启动技术和基于服务器的软件，所以您可在支持的计算机上远程安装 Windows 2000 Professional 的一个映像，从而避免了物理访问每台计算机来执行安装。必须确保每台计算机的硬件是兼容的并且安装了可引导的网卡。必须为一组计算机的特定配置设置一个不同的 RIS 映像。根据特殊用户或组策略设置的限制，安装过程中提供了一个安装选择列表。需要维护的 RIS 映像数量可能与组策略的数量相同。如果只有当所有配置都通用的安装选择是按照此方法进行安装时，这种情况才是有益的。

有关远程操作系统安装的详细信息，请参见本书中“应用更改与配置管理”，并请参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide* 中的“远程 OS 安装”。

RIS 服务器网络负载的影响

因为 RIS 服务器用来在客户计算机上安装操作系统映映像，该服务器产生的通信量与其他网络上作为软件安装点的服务器产生的通信量相似。通常，与提供应用程序和常规升级的多用途软件安装点的通信量相比，RIS 服务器的更容易预估。当许多用户加载映像（例如，新的操作系统映像部署期间或一组新的计算机加入网络时），RIS 产生的通信量会比较高。系统安装之后，每日通信量会降低。

通常的规则是，把 RIS 服务器放在所服务的客户计算机附近。这将使因此产生的网络通信本地化，并可降低它的影响。

如果环境需要下列过程之一，要保证在不影响其他应用程序的情况下优化这些过程：

- 频繁地重新安装操作系统，例如在教室中。
- 定期地安装大量的操作系统，例如在交付给用户之前预装所有的新系统。

对于教室的例子，要考虑把物理网络分段，并为每个教室或 RIS 服务器硬件可以支持的每组教室提供一个专用的 RIS 服务器。

对于预装的例子，要考虑创建预装实验室，在此可用高速网络和 RIS 服务器硬件大批量处理计算机，从而减少安装时间。

优化性能

因为远程操作系统安装主要是文件复制过程，所以 RIS 服务器通常的性能因素与其他文件输入/输出 (I/O) 密集服务器（例如 Web 服务器及文件和打印服务器）类似。这些因素包括服务器磁盘吞吐量和网络带宽。优化 RIS 服务器的性能时，要评估这些因素和或许会存在于 RIS 服务器及其服务的客户之间网络上的其他约束。当 RIS 服务器及其网络连接过载时，结果是客户计算机的安装时间和最初文件复制阶段的 TFTP 超时的增加。

DHCP 和 DHCP 服务器

因为远程操作系统安装程序（启用 PXE）的客户使用 DHCP 发现机制获取网络地址、定位 RIS 服务器，所以在确定 RIS 服务器布局策略时，单位中 RIS 与 DHCP 之间的关系起关键的作用。

在简单的环境中，向每一个使用中的 DHCP 服务器添加 RIS 是通用的解决方案。当使用 Windows 2000 DHCP/RIS 组合服务器的方案时，RIS 客户与 DHCP 和 RIS 服务器之间传递的初始网络数据包的数目减少了，并且初始服务器的响应也变得更快。此外，Windows 2000 DHCP/RIS 组合服务器总是一起应答客户。这样，通过利用把客户计算机向 DHCP 服务器聚合的现存规划，提供了一种简单形式的负载平衡，并且简化了疑难解答和管理的步骤。

尽管 RIS 服务器必须放在客户计算机附近，还会产生大量网络负载，因而常常要求服务器具有高端硬件，但 DHCP 服务器却恰恰相反。DHCP 产生相对少得多的通信量，通常不需要高端服务器硬件，而且有时是集中放置而不是接近客户计算机。因此，您也许发现简单地把 RIS 加入现有的 DHCP 服务器是不切实际的。这种情况下，您也许想把 RIS 服务加入现有的软件安装点服务器，因为它们有与 RIS 服务器类似的规划和布局需求；或者要让 RIS 服务器独立于其他支持服务器。

当 RIS 服务器从 DHCP 服务器中分离出来，或者使用非 Windows 2000 DHCP 服务器时，控制哪个 RIS 服务器响应特定客户就成了要首先考虑的问题。这是因为基于 PXE 的远程启动过程不提供决定客户从哪一个服务器接受服务的方法。有关控制这一过程方法的详细信息，请参看本章后的“控制 RIS 服务器选择和平衡负载”。

无论采用何种方法组合 DHCP 和 RIS 服务器，作为防止未经授权的服务器为网络上的客户提供服务的一种方法，每个 RIS 服务器都必须在 Active Directory 中授权。对 RIS 和 Windows 2000 DHCP 服务器的授权过程通过 Microsoft 管理控制台中的 Windows 2000 DHCP 管理单元进行。这一过程与组合或分离 RIS 和 DHCP 服务器或使用 Windows DHCP 没有直接关系。Windows 2000 DHCP 管理单元只是作为一种验证机制而被重复使用，并且，即使不安装 DHCP 服务，也可在任何安装了管理工具包的基于 Windows 2000 的计算机上运行。

警告 不要只为了获取该管理单元而试图在 RIS 服务器上安装 Windows 2000 DHCP。要为 RIS 客户提供服务，任何 Windows 2000 DHCP 和 RIS 的组合都必须有功能完全正常的 DHCP 服务（包括定义的和活动的范围）。这是因为组合服务器上的 Windows 2000 DHCP 服务可以感知 RIS 的安装。如果一个客户机在它的 DHCP 发现广播中说明它需要 DHCP 和远程启动服务，DHCP 就会发送一个回复，回复中包含 DHCP 和那个服务器远程启动的特定详细信息。如果服务器上的 Windows 2000 DHCP 服务不能正确地应答客户，那么服务器就不能产生远程启动回复。

控制 RIS 服务器选择和平衡负载

默认地，基于 PXE 的客户机广播它的服务请求时，所有接受到请求的服务器都会应答。第一个应答的服务器就是提供服务的服务器；组合 DHCP/RIS 服务器的响应比独立服务器的响应更受到优先考虑。当客户可用多个服务器时，尽管这为防止客户使用不恰当的服务器提供了必要的负载平衡，但通常最好限定哪一个服务器应答特定的客户机。例如，有这样一个服务器，它对客户机来讲是属于本地的，当客户机请求服务时可能很繁忙或出现故障。

控制服务器选择的第一种方法是物理地控制网络路由，从而只在合适时转发 DHCP 广播。这种方法物理地允许只有获准接收客户服务请求的 DHCP/RIS 服务器才会应答。如果 DHCP/RIS 服务器在网络上与客户机的位置相近，此方法可能是很好选择。

为了适应多种不同的场景，远程操作系统安装程序为控制服务器选择提供了额外的功能。这些功能涉及到配置 Active Directory 中的客户计算机帐户，以便使用一个特定的 RIS 服务器，此过程称为“前期部署”。既可在现存的计算机帐户上进行前期部署，也可在系统加入域前创建新计算机帐户时进行。当 RIS 服务器应答客户机的服务请求时，服务器会检查 Active Directory（整个森林），看是否存在带全局唯一标识符（GUID）的计算机帐户，该 GUID 应与服务请求所包含的 GUID 相匹配。如果找到匹配的计算机帐户，还要检查该帐户是否已配置成使用某一特定的 RIS 服务器。如果是这样，即便计算机帐户所指定的 RIS 服务器与最初向客

户机提供回复的服务器不同，给客户机的回复中也总是提供该 RIS 服务器。这称为“服务器推举”，并且无论是哪一个特定的 RIS 服务器回复了客户机最初的服务请求，它都提供了一种简单方法，用于控制最终哪个 RIS 服务器向特定的客户计算机提供操作系统安装服务。

要允许使用其他的灵活性和安全，还可把前期部署和推举的概念与 RIS 服务器设置（用于控制服务器怎样响应客户）结合在一起。每一个 RIS 服务器有两个设置：“响应客户计算机的服务请求”和“不响应未知客户计算机”。通过前期部署所有的计算机帐户，以及有选择地控制哪一个 RIS 服务器配置成应答客户机，服务器可变为专用于回复客户服务请求和提供适当的推荐，或者向客户机提供实际的远程操作系统安装服务。

图 25.3 描绘了如何在客户计算机与 RIS 服务器之间建立关联的示例。

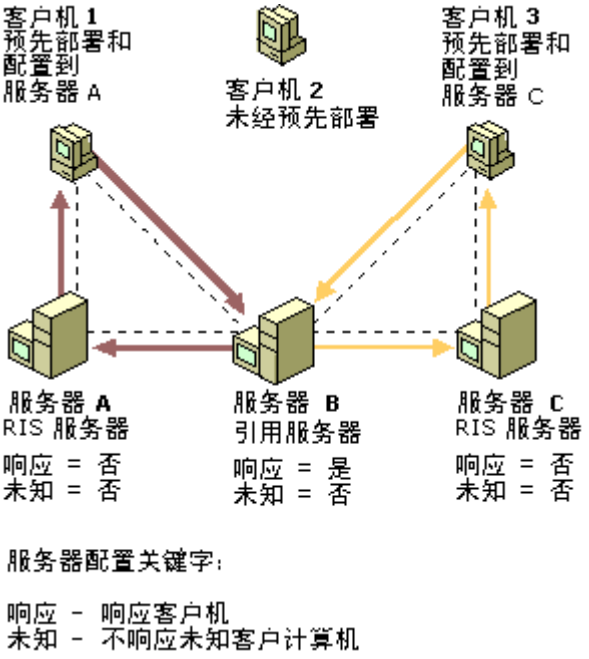


图 25.3 客户计算机与 RIS 服务器建立关联的示例

在图 25.3 中，只有服务器 B 会应答请求服务的客户计算机。因为客户计算机 1 和 3 已预先部署和配置为从特定的 RIS 服务器获取服务，所以它们会收到一个回复，把它们引向适当的服务器（A 或 C）。如果合适的话，可以创建多个类似服务器 B 的专用推举服务器，它们都使用 Active Directory 中的计算机帐户来确定要进行的恰当的推举。

- 服务器 A 和 C 肯定不会回复最初的客户服务请求，但是通过推举，这些服务器可为客户机提供实际的操作系统安装服务。然后您就可决定是否在推举服务器（服务器 B）上选择“不响应未知客户计算机”配置选项。选择这一选项可确保：服务器 B 只回复经过预先部署的客户计算机。

- 如果任何客户被配置为只从 服务器 B 接受服务，则该服务器事实上会成为专用的推举服务器，或者还提供实际的操作系统安装服务。

如果没有选择“不响应未知客户计算机”选项，服务器 B 会把自身作为远程启动服务器，回复来自未经预先部署客户机（例如客户机 2）的服务请求。

无论是否使用推举服务器，选择“不响应未知客户计算机”都提供了一种安全方案，防止未经预先部署的客户计算机从 RIS 服务器上进行操作系统安装。而且，并非所有提供解决方案的供应商（基于与远程操作系统安装程序相同的远程启动协议）都会提供控制回复何种客户服务请求的选项。通过使用预先部署和限制所有的 RIS 服务器响应已知的客户计算机，您可以在包含其他远程启动产品的网络上实现远程操作系统安装，而不会受到干扰。

使用路由器

因为客户服务请求基于 DHCP 发现过程，所以，把网络配置成支持跨路由器执行远程操作系统安装，其要求与跨路由器支持 DHCP 相同。

配置成转发 DHCP 广播的路由器会自动转发客户服务请求；但是除 DHCP 服务器外，必须确保请求被转发到适当的 RIS 服务器中。根据路由器的使用模式，DHCP 广播转发的特定路由器配置有可能由一个子网（或路由器接口）或一个特定主机支持。如果使用 Windows 2000 DHCP，但 RIS 服务器在另一台计算机上，或者使用非 Windows 2000 DHCP，则必须确保路由器把 DHCP 广播转发到 DHCP 和 RIS 服务器上。否则，客户机将收不到对远程启动请求的回复。

由于安装操作系统涉及到的网络通信量，请仔细考虑 RIS 服务器的放置位置以及如何使用预先部署和推举服务器来适应现有的网络设计，从而使客户机安装的影响降到最低。

安装配置示例

这里的示例提供了很多过程，用于在已有客户配置或没有任何现存配置的计算机中安装 Windows 2000 Professional。

现有客户计算机

此节中的示例用于有以下预先存在的客户配置的计算机。

例 1：带有 Windows 2000 兼容客户应用程序的 Windows NT Workstation 4.0

进行升级。可以升级的客户操作系统包括 Windows 95、Windows 98、Windows NT、Workstation 4.0 和 Windows NT Workstation 3.51。

有关与 Windows 2000 Professional 兼容应用程序的详细信息，请参见 Web 资源页的 Directory of Windows 2000 Applications 链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources。

要在有兼容硬件的计算机上安装 Windows 2000 Professional

1. 备份用户设置。

   用以下方法之一升级系统：

   执行以下操作，开始“推”（全自动）安装：

   - 使用系统管理软件例如 Microsoft® System Management Server。

   – 或 –

   - 执行网络安装。

   – 或 –

   - 执行远程启动。这需要配置远程安装服务器和安装好的可引导网卡。

   开始执行本地安装的方法是：从命令行运行带有恰当参数的 Winnt32.exe，并且：

   - 执行手动安装（无应答文件），应答所有提示。

– 或 –

- 使用应答文件进行自动或半自动安装。在全自动安装中，应答文件为所有问题提供应答。也可用半自动安装，使您选择的应用程序能够有一些用户输入。

要在有不兼容硬件但不需要替换硬盘的计算机上安装 Windows 2000 Professional

1. 更换除硬盘以外的所有必需硬件。
2. 验证所有新硬件运行正常。
3. 备份用户设置。

   可用以下方法之一升级系统：

   执行下列操作，开始“推”（全自动）安装：

   - 使用系统管理软件例如 Microsoft System Management Server。

     – 或 –

   - 执行网络安装。

     – 或 –

   - 执行远程启动。这需要配置远程安装服务器和安装好的引导网卡。

   开始执行本地安装的方法是：从命令行运行带有恰当参数的 Winnt32.exe，并且：

   - 执行手动安装（无应答文件）。应答所有提示。

     – 或 –

   - 执行自动或半自动安装。

要在有不兼容硬件且必需替换硬盘的计算机上安装 Windows 2000 Professional

至少升级下列组件之一：

- RAM
- 处理器

2. 验证所有新硬件运行正常。
3. 备份用户设置。

   备注 尽管升级计算机前把整个硬盘的内容备份到一个新硬盘是可能的，但对客户计算机来说这通常是不现实的。

4. 更换硬盘。复制所备份的映像。

   可用下列方法之一，从命令提示运行带所需参数的 Winnt.exe：

   - 执行手动安装（无应答文件），然后应答所有提示。

     – 或 –

执行自动或半自动安装。可用下列方法之一：

- CD-ROM 引导安装。
- Syspart。这在计算机上安装新硬盘时很有用。
- Sysprep。在相同的计算机（HAL 和大型存储设备控制器必须相同）上安装时使用。
- 远程启动. 这需要配置远程安装服务器且已安装引导网卡。

5. 安装与 Windows 2000 Professional 兼容的应用程序。
6. 验证系统按要求运行。
7. 导入用户设置（例如，Regedit/Regedt32、登录脚本、策略、漫游配置文件）。

例 2：Windows NT Workstation 3.5 或早期版本，及非 Microsoft 客户计算机

无法升级的客户操作系统包括 MS-DOS、Windows 3.x、Windows NT Workstation 3.5 或更早版本，以及 OS/2。

要进行全新安装，先取得由 OEM/Solution Provider 生产的计算机。要在一个新计算机上进行全新安装或为现有计算机安装操作系统，执行下列步骤。

备注 有关与 Windows 2000 兼容应用程序的详细信息，请参见 Web 资源页的 Directory of Windows 2000 Applications 链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources。

要在不能升级的客户操作系统上安装 Windows 2000 Professional

1. 备份用户设置。

   警告 如果在运行不能升级到 Windows 2000 的操作系统的计算机上安装 Windows 2000 Professional，所有的用户时置都会丢失。

   可用下列方法之一，从命令提示运行带所需参数的 Winnt.exe：

   - 执行手动安装（无应答文件），然后应答所有提示。

     – 或 –

     执行自动或半自动安装。可用下列方法之一：

     - CD-ROM 引导安装。
     - Syspart。这在计算机上安装新硬盘时很有用。
     - Sysprep。在相同的计算机（HAL 和大型存储设备控制器必须相同）上安装时使用。
     - 远程启动。这需要配置远程安装服务器且已安装引导网卡。

2. 安装与 Windows 2000 Professional 兼容的应用程序。
3. 验证系统按要求运行。

4. 导入用户设置（例如，Regedit/Regedt32、登录脚本、策略、漫游配置文件）。

新客户计算机

未安装任何 Windows 2000 以前版本操作系统的计算机需要执行 Windows 2000 Professional 全新安装。

要准备安装，需先取得由 OEM /解决方案提供商生产的计算机。

要在尚未安装任何 Windows 2000 以前版本操作系统的计算机上安装 Windows 2000 Professional

- 执行手动安装（无应答文件），然后应答所有提示。

  – 或 –

  执行自动或半自动安装。请使用下列方法之一：

- CD-ROM 引导安装。
- Syspart。这在计算机上安装新硬盘时很有用。
- Sysprep。在相同的计算机（HAL 和大型存储设备控制器必须相同）上安装时使用。
- 启动磁盘并用应答文件运行安装程序。
- 远程启动。这需要配置远程安装服务器和安装好的可引导网络适配器。

安装任务列表

表 25.7 是安装 Windows 2000 Professional 和所需的应用程序时涉及的任务摘要。

表 25.7 安装任务摘要

任务	本章中的位置
解决关键规划问题。	解决关键规划问题
创建分发文件夹。	准备安装
检查应答文件	检查应答文件
检查 Windows 2000 安装命令	准备安装
基于关键规划选择应用程序安装方法。	客户应用程序的自动安装
基于关键规划选择操作安装方法。	Windows 2000 Professional 的自动安装

附录 A - 规划表示例

在部署 Microsoft® Windows® 2000 时可能需要规划和协调几个部署项目。您可以使用本附录提供的规划表用最经济、最有效的方式为单位部署 Windows 2000。

使用部署规划表将有助于熟悉自己单位的特殊 IT 需求和 Windows 2000 中能够帮助满足这些需求的特性。填表之前应先阅读与工作表有关的章节。这些章节引入新的概念并提供基本的信息，这些概念和信息将有助您最佳地利用规划表。

本附件内容

使用本附录

本附录中的工作表是按对应的章节标题组织；但是，并非每一章都有一个工作表且有些章节有多个工作表。表 A.1 列出具有工作表的章节并显示这些工作表在本附录中出现的顺序。

表 A.1 本附录中的工作表

章节和工作表名称	章节序号
Windows 2000 部署规划简介	第 1 章
管理基础结构服务	
桌面管理解决方案	
安全特性	
信息发布与共享	
组件应用程序服务	
可扩展性和可用性	
网络和通讯	
存储管理	
建立 Windows 2000 测试实验室 记录每次测试的范围和目标 跟踪测试结果	第 4 章
为 Windows 2000 准备网络基础结构	第 6 章
确定域迁移策略 记录迁移目标 当完成域迁移任务时记录	第 10 章
规划分布式安全 确定潜在的安全风险	第 11 章
服务器自动安装与升级	第 13 章

决定何时何地使用自动安装方法 当完成安装任务时记录	
升级和安装成员服务器 成员服务器规划表 服务器数据备份和灾难恢复规划 确定新的硬件要求 记录服务器规格 计划升级或全新安装	第 15 章
确保应用程序和服务的可用性 明确高可用性需求 规划网络负载平衡	第 18 章
同步 Active Directory 与 Exchange Server 目录服务 建立连接协议 确定映射的目录对象 列出不映射的属性 建立目录同步日程安排 记录目录同步的联系人	第 20 章
测试应用程序与 Windows 2000 的兼容性 确定应用程序的优先级 规划和跟踪测试策略	第 21 章
定义客户管理与配置标准 确定用户的计算要求 定义客户支持问题 分配客户管理和支持任务 定义组策略要求	第 23 章
应用更改与配置管理 记录应用程序及其管理选项 为用户定义配置管理策略	第 24 章
自动执行客户安装与升级 记录自动安装方法 记录客户安装任务	第 25 章

重要 这些工作表还存在于 DPGDocs.doc 文件中，该文件在与《Microsoft® Windows® 2000 Server Resource Kit》一起的 CD 上。该 CD 包含这些工作表的一个版本，您可以在本单位内定制和打印这些工作表。

Windows 2000 部署规划简介

“Windows 2000 部署规划简介”一章包含对 Windows 2000 操作系统的功能和优点的高级介绍。以下的工作表列出 Microsoft® Windows® 2000 Server 和 Microsoft® Windows® 2000 Professional 的主要功能。阅读本书中的这些章节时，使用这些工作表将有助于确定 Windows 2000 的主要功能以及这些功能如何满足自己单位的商业需要。当检查这些功能时，应考虑单位的短期和长期目标。

表格的格式允许输入对这些功能在单位中的潜在角色的注释。利用这些工作表对本单位需要的 Windows 2000 功能定制一份实行概要。

备注 以下表格只重点列出 Windows 2000 Server 和 Windows 2000 Professional 的主要优点，并非所有功能的完整描述。有关某个特定功能的详细信息，请参见产品的帮助文件或《Microsoft® Windows® 2000 Server Resource Kit》中的相应卷和章节。

管理基础结构服务

Windows 2000 Server 的管理基础结构服务为 IT 部门提供了一些工具，使用这些工具可以提供最高级的服务并降低拥有成本。表 A.2 描述了 Windows 2000 Server 的管理基础结构服务及其优势。

表 **A.2** 管理基础结构服务

功能	该功能在本单位中的角色
目录服务 Microsoft® Active Directory™ 存储网络上所有对象的信息，使这些信息易于寻找。提供灵活的目录层次结构、细化的安全设置委派、高效的权限委派、集成的 DNS、高级的编程接口以及可扩展的对象存储。	
管理服务 Microsoft® 管理控制台 (MMC) 让系统管理员用一个公用控制台监视网络运行状况和使用管理工具。对于由 IT 支持和管理部门的某个成员所完成的任务，MMC 是可以完全自定义的。	
组策略 组策略允许管理员定义和控制计算机和用户的状态。组策略可在目录服务的任意层次设置，包括站点、域和组织单元。还可根据安全组成员身份筛选组策略。	
规范服务 通过使用 Windows 管理规范 (WMI)，管理员可关联多个源的数据和事件，这些源可位于本地或整个组织。	
脚本服务 Windows 脚本主机 (WSH) 支持从用户界面或命令行直接执行 Microsoft® Visual Basic® Script、Java 和其他脚本。	

有关设计和部署 Windows 2000 目录服务和组策略的详细信息，请参见本书的“设计 Active Directory 结构”、“规划分布式安全”、“定义客户管理与配置标准”和“应用更改与配置管理”。

桌面管理解决方案

桌面管理方案的功能可让您更加容易地安装、配置和管理客户计算机，从而降低单位的总体拥有成本。表 A.3 重点列举了 Windows 2000 Server 和 Windows 2000 Professional 中可以提高用户生产力的桌面管理功能。

表 A.3 桌面管理解决方案

功能	该功能在本单位中的角色
IntelliMirror Microsoft® IntelliMirror™ 这一组功能可以使用户在单位内部使用不同计算机时，其数据、应用程序和自定义的操作系统设置会如影跟随。	
Windows 安装程序 Windows 安装程序控制软件的安装、修改、修复和删除。它为打包安装信息提供了一个模型并为与 Windows 安装程序协同使用的应用程序提供了 API。	

远程安装 基于 DHCP 的远程启动技术可以从一个远程地点把操作系统安装到客户的本地硬盘上。网络启动可由以下几种方式进行：预启动运行 (PXE) 环境、启用了 PXE 的网卡、特定的功能键或为没有 PXE 客户提供的远程启动软盘。	
漫游用户配置文件 漫游用户配置文件可把注册表值和文档信息复制到网络上的某一位置，这样无论用户在何处登录，用户的设置都是可用的。	
选项组件管理器 Windows 2000 Server 安装程序通过一个安装模块让您可以在安装系统过程中或之后捆绑和安装附件。	
磁盘复制 您可自定义安装一台 Windows 2000 Server 或 Windows 2000 Professional，然后把它克隆到相似的计算机上。	

备注 您可使用 Microsoft® Systems Management Server (SMS) 来辅助 Windows 2000 的桌面管理技术。

有关部署 Windows 2000 Server 和 Windows 2000 Professional 管理方案的详细信息，请参见本书中的“ 定义客户管理与配置标准 ”和“ 应用更改与配置管理 ”。

安全功能

企业级的安全设置既要灵活，又要有力，这样管理员才能在配置规则、满足安全需求的同时，不会防碍必要信息的自由流动。表 A.4 着重列举了 Windows 2000 的安全功能。

表 A.4 安全功能

功能	该功能在本单位中的角色
安全模板 管理员可以设置不同的全局和本地安全设置，包括安全敏感的注册表值；对文件和注册表的访问控制；系统服务的安全设置。	
Kerberos 身份验证 Windows 2000 域内部或域间的基本安全协议。支持客户和服务器相互的身份验证，支持通过代理机制进行委派和授权。	
公钥基础结构 (PKI) 可使用集成 PKI 在多种 Windows 2000 Internet 和企业服务上，包括基于外部网的通讯，实现有力的安全机制。	
智能卡基础结构 Windows 2000 包括了一个标准模型，用来将智能卡阅读器、卡和计算机连接起来，还包括了独立于设备的 API 以启用支持智能卡的应用程序。	
网际协议安全 (IPSec) 管理 IPSec 支持网络级身份验证、数据完整性和对内部网、外部网和 Internet Web 加密来保证	

安全。	
NTFS 文件系统加密 基于公钥的 NTFS 可以针对单个文件或目录启用。	

有关部署 Windows 2000 安全服务的详细信息，请参见本书的“规划分布式安全”和“确定 Windows 2000 网络安全性策略”。

信息发布与共享

Windows 2000 中的信息发布和共享技术使得您可以更方便地通过 Internet、内部网和外部网来共享信息。表 A.5 着重列举了信息发布和共享的功能。

表 A.5 信息的发布和共享

功能	该功能在本单位中的角色
集成的 Web 服务 Windows 2000 Server 集成的 Web 服务可让您使用许多 Web 发布协议。	
索引服务 集成的索引服务可让用户在不同格式和语言的文件中进行全文搜索。	
可移动存储 包括服务器和工具组件，可通过网络提供音频、视频、图示音频和其他多媒体形式。	
打印 Windows 2000 把域内所有可用的共享打印机放在 Active Directory 中。	

有关部署 Windows 2000 信息发布和共享服务的信息，请参见本书中的“升级和安装成员服务器”和《Microsoft® Windows® 2000 Server Resource Kit Internet Information Services Resource Guide》。

组件应用程序服务

作为一个开发平台，Windows 2000 支持组件对象模型 (COM) 和 分布式 COM (DCOM)，这样开发人员能够更高效地创建更多可扩展的基于组件的应用程序。表 A.6 着重列举了组件应用服务的功能。

表 A.6 组件应用服务

功能	该功能在本单位中的角色

队列组件

开发人员和管理员可在部署时选择合适的通讯协议（DCOM 或异步）。	
发行和预订 COM 事件为所有 Windows 2000 Server 应用程序提供了统一的发行和预订机制。	
事务服务 通过呼叫大型机上的应用程序或从消息队列发送或接收消息来提供信息更新。	
消息队列服务 保证消息事务或者完成或被安全地退回到企业	

环境。	
Web 应用程序服务 开发人员可用 Active Server Pages 对已有的基于服务器的应用程序建立基于 Web 的前端。	

有关部署 Windows 2000 组件应用服务和 Microsoft 安全支持提供商接口的更多信息，请参见本书的“确定 Windows 2000 网络安全性策略”。有关供开发人员使用的详细信息，参见 Web 资源页的 MSDN Platform SDK 链接，地址是：
http://windows.microsoft.com/windows2000/reskit/webresources。

备注：您可与应用程序开发组人员讨论这些功能及其潜在的商业价值。他们的专业知识会有助于判定这些技术对单位的潜在商业价值。

可扩展性和可用性

一段时间内，更快的 CPU 和网卡曾经是传统的网络性能判断基准。将来，更有效的读/写能力、增强的输入/输出 (I/O) 性能和更快的磁盘访问将会是网络结构中同样重要的特性。需要关键任务计算机的环境现在可以使用 Windows 2000 的扩展功能。表 A.7 着重列举了 Windows 2000 中协助您提高网络可扩展性和可用性的功能。

表 A.7 可扩展性和可用性

功能	该功能在本单位中的角色
企业内存结构	
Windows 2000 Advanced Server 允许访问处理器上高达 32 GB 的内存。	
增强的对称多重处理 (SMP) 可扩展性 Windows 2000 Advanced Server 已针对 8 路 SMP 服务器进行了优化。	
群集服务 两个或更多服务器可以作为单一系统一起工作。	
智能输入/输出 (I2O) 支持 I2O 使主机的主要 CPU 不必处理中断频繁的 I/O 任务。	
终端服务 通过终端仿真，终端服务允许相同的应用程序运行在不同类型的客户硬件上，包括瘦客户机、早期的计算机或不运行 Windows 的客户机。该服务也可作为一个远程管理选项。	
网络负载平衡 可以把多达 32 台运行 Windows 2000 Advanced Server 的服务器组合成一个负载平衡的群集。常用于在其群集的 Internet 服务器应用程序间分发传入的 Web 请求。	
IntelliMirror IntelliMirror 让用户不连接到网络时，也可携带自己的数据、应用程序和设置。	

有关部署 Windows 2000 群集服务的详细信息，请参见本书的“确保应用程序和服务的可用性”。

有关终端服务的更多信息，请参见本书的“部署终端服务”。

网络和通讯

要想改善您的网络环境，请考虑表 A.8 中所列的 Windows 2000 技术，这些技术能提供更多的带宽控制、安全的远程网络访问和对新一代通讯方案的本机支持。

表 A.8 网络和通讯

功能	该功能在本单位中的角色
DNS 动态更新协议	
不必再手动编辑和复制 DNS 数据库。	
服务质量（QoS） QoS 协议和服务为 IP 通信提供了一个有保障的、端到端的快速传递系统。	
资源保留协议（RSVP） 该信令协议允许发件人和收件人建立一条专用路径，按指定的服务质量进行数据传输。	
异步传输模式（ATM） ATM 网络可以同时传输大量的网络通信，包括声音、数据、图像和视频。	
数据流媒体服务 在网络上传递多媒体文件的服务器和工具组件。	
光纤信道 通过在一个连接中映射公用的传输协议并合并网络和高速输入输出，光纤信道可以提供 1 Gbps 的数据传输速度。	
IP 电话服务 电话服务 API 3.0 (TAPI) 综合了 IP 和传统的电话服务。	

有关 Windows 2000 网络和通讯功能的详细信息，请参见本书中的“为 Windows 2000 准备网络基础结构”和“确定网络连接策略”。

存储管理

Windows 2000 Server 提供的存储服务既能提高可靠性，又能改善用户访问。表 A.9 着重列出了这些服务。

表 A.9 存储管理

功能	该功能在本单位中的角色
远程存储	
监视本地硬盘上的可用空间数量。当主硬盘上的可用空间降到可靠运行所需的水平之下时，远程存储会删除已复制到远程存储器的本地数据。	
可移动存储 管理员可以管理可移动存储设备和功能。管理员可以创建由一个给定应用程序拥有和使用的媒体池。	
NTFS 文件系统增强	

支持性能增强功能，如文件加密、无须重新启动即可在 NTFS 卷中添加磁盘空间、分布式链接跟踪以及通过每个用户的卷配额来监视和限制磁盘空间使用。	
磁盘配额 有助于管理员规划和实施磁盘的使用。	
备份 通过备份，用户可以把数据备份到不同的存储媒体，包括硬盘驱动器、磁性和光媒体。	
分布式文件系统（Dfs）支持 管理员可以创建一个目录树，包括多个文件服务器和文件共享，Windows 2000 客户可以和任何有匹配协议的文件服务器实现互操作。	

有关部署 Windows 2000 Server 存储管理技术的详细信息，请参见本书的“确定 Windows 2000 存储管理策略”。

建立 Windows 2000 测试实验室

本书中的“建立 Windows 2000 测试实验室”一章强调了全面进行基于实际方案的测试的重要性。还提供了许多指导方针，这有助于建立本单位的实验室和运行全面的测试程序。

启动时需要：

- 创建一个描述范围、目标和方法的测试计划。
- 设计测试案例以描述测试方案和需要处理的问题。
- 实施测试并评估结果。
- 记录测试结果。
- 将暴露出的问题送给有关人员解决。

您的实验室需要尽可能地仿真实际的工作环境。以下部分是测试规划中应当记录的基本组件：

- 当前的网络设计（逻辑的和物理的）。
- Windows 2000 设计建议。
- 待评估和仔细研究的功能列表。
- 现有的硬件的清单（服务器、客户计算机和便携式计算机）。
- 建议用于 Windows 2000 的硬件列表。

  这个列表可能在测试期间有所扩充，但需要一个初始列表来装备实验室。
- 管理工具的列表（Windows 2000、第三方和自定义工具）。
- 需要安装以用于 Windows 2000 的升级的列表，例如服务包、驱动程序、基本输入输出系统（BIOS）等。

在实验室说明中还包含下列类型的信息：

域结构，包括：

- 目录林和目录树层次结构。
- 组策略对象（设置以及在何处应用）。
- 每个域的目的。
- 填充用户帐户数据的方法。
- 信任关系（可传递的和明确的）。

域控制器，包括：

- 如果是从 Windows NT 4.0 版本迁移过来的，主域控制器 (PDC) 和备份域控制器 (BDC)。
- 如果是从其他操作系统迁移过来的，将要提升为域控制器的服务器。

- 成员服务器，包括将在服务器上面运行的服务。

客户计算机，包括：

- 计算机构造和型号。
- 内存数量。
- 处理器类型和速度。
- 硬盘容量。
- 图形卡（类型、分辨率和色度）。

用于特定测试的实验室设计的使用，包括：

- 混合模式和本机模式测试。
- 拨号和其他远程测试。
- 互操作性测试（UNIX、主机和其他系统）。
- 复制和 Active Directory 站点测试。
- WAN 链接测试。

使用表 A.10 来记录每一个测试的范围和目标。为每一个测试完成一个新表。

表 A.10 记录每一个测试的范围和目标

测试标识符：	**测试日期：**
	测试范围和目标：
测试的目的	
特殊硬件要求。	
特殊软件要求	
特殊配置要求	
所使用的测试过程	
预期结果或成功标准	

表 A.11 列出了跟踪表的类型，跟踪表用于监视测试的进度和保证所有后续问题都得到处理。

表 A.11 跟踪测试结果

测试标识符	测试日期	结果	操作项目

为 Windows 2000 准备网络基础结构

本书中的“为 Windows 2000 准备网络基础结构”一章为记录现有网络基础结构提供了建议。它还有助于确定网络基础结构的范围，比如在部署 Windows 2000 前可能需要升级或修改的服务器、路由器和网络服务。

为部署 Windows 2000 做网络准备时，应该记录当前网络环境中的下面几项：

- 硬件和软件
- 网络基础结构
- 文件、打印和 Web 服务器
- 业务线应用程序
- 目录服务结构
- 安全性

应当全面记录以下与硬件有关的项：

- 路由器。
- 打印机。
- 调制解调器。
- 其他硬件，如独立磁盘冗余阵列（RAID）以及路由和远程访问服务（RRAS）服务器硬件。
- 基本输入/输出系统（BIOS）设置。
- 驱动程序版本及其它软件和固件信息。

软件清单应包括：

- 在所有计算机上发现的所有应用程序。
- 与这些应用程序有关的动态链接库的版本号码（或日期和时间戳数据）。

- 已经应用于操作系统或应用程序的服务包。

还应记录下服务器和客户计算机的网络配置。该信息位于控制面板中的网络选项中，包括：

- 标识
- 服务
- 协议
- 适配器
- 绑定
- Internet 协议地址

您需要记录：

- 网络的逻辑单位
- 名称和地址解析方法
- 所使用的服务的配置
- 网络站点所处位置
- 站点间的有效带宽

还需要收集尽可能多的此类信息来创建物理和逻辑的网络图表，该图表可用于在网络图象形成之前和之后与他人讨论。有关所记录的重要技术问题的详细信息，请参见本书的“为 Windows 2000 准备网络基础结构”。

确定域迁移策略

为了规划从 Windows NT 到 Windows 2000 的域结构迁移，必须首先决定迁移目标。这些目标可能会主动定位您所关注的部署问题，如对生产系统和系统性能的潜在损坏和延长平均无故障时间的方式。迁移目标还会影响测试规划和接受标准。

阅读“确定域迁移策略”一章并使用这些工作表开始规划迁移策略。使用一个类似 A.12 的表来记录本单位特定的迁移目标。该表提供目标示例以方便您开始。

表 A.12 记录您的迁移目标

目标	完成目标的指导
使对生产环境的损坏最小化	• 维持迁移时和迁移后用户对数据、资源、和应用程序的访问。
维持系统性能。	• 维持迁移时和迁移后用户熟悉的环境。 • 维持迁移时和迁移后用户对数据、资源、和应用程序的访问。
延长平均无故障时间	• 维持迁移时和迁移后用户熟悉的环境。 • 维持迁移时和迁移后用户对数据、资源、和应用程序的访问。
使管理的开销最小化	• 维持迁移时和迁移后用户熟悉的环境。 • 提供用户帐户的无缝迁移。 若有可能，用户必须能够保留他们的密码。 • 尽量减少管理员对客户计算机的访问次数。

	• 尽量减少新的资源使用权限的数量。
使“ quick Wins ”最大化	• 首先部署主要功能。
维护系统安全。	• 部署时总保持一个安全的系统。 • 建立一个部署安全策略。

使用表 A.13 来记录完成每一任务的日期。

表 A.13 当完成域迁移任务时记录

任务	完成日期
确定迁移路线图。	
确定受支持的升级途径。	
检查现有域结构。	
制定恢复规划。	
确定升级域控制器的策略。	
确定升级域的顺序。	
确定切换到本机模式的时间。	
确定重组域的理由。	
确定重组域的时间	
移动用户和组。	
移动计算机。	
移动成员服务器。	
建立信任。	
克隆安全负责者。	
切换到本机模式。	

规划分布式安全

为实现总体的安全策略，您需要对计算机网络中的多个安全功能进行协调。使用表 A.14 来记录本单位的安全性的各个方面。比如说安全风险，请参阅本书的“ 规划分布式安全 ”一章。列出您单位特定（而非一般）的安全风险。在迁移策略中，填入本书中所有与安全有关的章节的细节，包括"规划公钥基础结构 ”和“ 确定 Windows 2000 网络安全性策略 ”。

表 A.14 确定潜在的安全风险

潜在的安全性风险	描述	迁移策略（包括策略、Windows 2000 功能和其他技术方案）

服务器自动安装与升级

在自动安装 Windows 2000 Server 之前，您需要决定是从 Windows NT 升级还是执行一个全新安装。“ 服务器自动安装和升级 ”一章将帮助您决定采用何种安装方式。以下问题的设计目的是方便您开始做决定。

1. 您单位目前是否有一个正在使用的 Windows NT 管理安装？是 □ 否 □
2. 是否计划使用现有的硬件和软件应用程序？是 □ 否 □

   如果对问题 1 和 2 的回答为是，推荐的方式为升级。

3. 是否计划在新的硬件上安装 Windows 2000？是 □ 否 □
4. 是否计划安装新的为 Windows 2000 环境编写的应用程序？是 □ 否 □

   如果对问题 3 和 4 的回答为是，推荐的方式为全新安装。

使用表 A.15 来决定使用何种自动安装方法和在单位内的何处使用这些方法。

表 A.15 决定何时何地使用自动安装方法。

方法	使用时间	使用该方法？	何时何地？
Syspart	拥有不同硬件的计算机的全新安装。		
Sysprep	主控计算机和目标计算机有相同硬件（包括硬件抽象层 (HAL) 和海量存储器设备）时使用。		
Systems Management Server (SMS)	用于对多个系统执行 Windows 2000 Server 的管理升级，特别是在这些系统地点分散时。		
可引导 CD	在基本输入/输出系统 (BIOS) 允许从可引导 CD-ROM 启动的计算机上使用。		

使用表 A.16 作为一个需要完成的任务和完成日期的检查表。

表 A.16 记录何时完成安装任务

任务	完成日期
解决关键规划问题。	
创建分发文件夹。	
检查应答文件。	
检查 Windows 2000 安装命令。	
基于关键规划选择应用程序安装方法。	
基于关键规划选择操作系统安装方法。	

升级和安装成员服务器

使用下列工作表与“ 升级和安装成员服务器 ”有助于决定最节省开支又行之有效的方式在本单位升级和安装 Windows 2000 成员服务器。当计划 Windows 2000 Server 升级或全新安装时，首先为每一个成员服务器定义规格。

在开始升级或全新安装前需要现有网络的图表。如果没有现有网络图表，创建一个然后开始为成员服务器的新安装或升级准备规划。

其次，确定单位是否已经决定安装和运行 Windows 2000 Active Directory。为了使用操作系统内几个高级服务，需要运行 Active Directory。

然后决定单位内每种类型的成员服务器的数量：

- 文件服务器：_____
- 打印服务器：_____
- 应用程序服务器：_____
- Web 服务器： _____
- 传真服务器： _____
- 代理服务器：_____
- 路由和远程访问服务服务器：_____
- 数据库服务器：_____

现在，为现有环境中的每一个服务器填写成员服务器规划表。这个工作表有助于您为本单位内的每一个服务器决定其单独的升级路径。为每一个服务器确定优先次序后，就可以为升级或全新安装创建计划。

成员服务器规划表

使用下列可选特性描述现有环境中的每一个服务器。

服务器类型：

文件服务器 ☐ 打印服务器 ☐ Web ☐ 服务器 ☐ 代理服务器 ☐ 传真服务器 ☐

路由和远程访问服务器 ☐ 数据库服务器 ☐

应用程序服务器 ☐ 指定已经安装的应用程序：

_____

_____

成员服务器名称： _____

该服务器上存储了多少数据？ _____
有多少数据传入/传出该服务器？ _____

当前用户数量： _____

当前操作时间（小时）： _____

服务器规格：

是否该计算机系统列在 Microsoft Windows 硬件兼容性列表 (HCL) 中？是 ☐ 否 ☐

序列号： _____

是否对硬件进行修改？是 ☐ 否 ☐

如果是，列出细节： _____

_____

计算机系统供应商： _____

计算机系统模型： _____

计算机系统构造： _____

已安装的物理内存数量： _____

已安装的网卡类型：

以太网 ☐ 令牌环 ☐ FDDI ☐ ATM ☐
其他 _____

- 网络适配器是否列在 HCL 中？是 ☐ 否 ☐

已安装的 CD-ROM 驱动器类型： _____

列出所有即插即用设备：

_____ _____

_____ _____

与计算机连接的外部硬盘类型： _____

_____

硬盘分区和可用的空闲磁盘空间： _____

_____

是否使用独立磁盘冗余阵列 (RAID)？如果是，详细说明：软件 RAID ☐ 硬件 RAID ☐ 正在使用何种层次的 RAID？ _____

_____

该服务器上安装了以下软件类型中的哪一种？第三方网络服务 ☐ 病毒扫描程序 ☐ 其他客户软件 ☐

有关特定应用程序的已知问题的信息，请参见 Windows 2000 Server 操作系统 CD 上的版本说明文件 (relnotes.htm)。

在升级或进行全新安装之前卸载版本说明文件中提到的应用程序。

服务器数据备份和灾难恢复规划

升级前备份下列文件：

_____ _____

_____ _____

_____ _____

_____ _____

_____ _____

_____ _____

最大停机允许： _____

停机造成的可以测算的损失： _____

确定新的硬件要求

将要升级的成员服务器数量： _____

在升级或全新安装前用新硬件替换的成员服务器数量：
_____

需要升级的网络适配器数量： _____

网络适配器类型：

以太网 ☐ 令牌环 ☐ FDDI ☐ ATM ☐
其他 _____

计划数据量： _____

计划的用户数量： _____

计划的操作时间（小时）： _____

记录服务器规格

打印服务器

如果是打印服务器，决定以下部分：

- 准备打印的用户数量及他们生成的打印工作负载：
- _____
- 打印需求的类型（比如说，如果销售部门的用户需要打印彩色的小册子，就需要彩色打印设备）。
- _____
- _____
- 打印机所处的位置。打印机位置应方便用户取打印文档。使用表 A.17 为每一台打印服务器分配打印机。

表 A.17 分配打印服务器、打印机和它们的位置

打印服务器	打印名称	位置

是否已经安装了所有需要的打印驱动程序？是 ☐ 否 ☐

（从 Windows 2000 Server 操作系统 CD 或打印机生产商那里获得打印驱动程序。）

网络上的客户是否运行第三方操作系统？

Macintosh ☐ NetWare ☐ UNIX ☐ 其他 ☐

必须在打印服务器上安装附加服务并为运行第三方操作系统的客户安装适当的打印驱动程序。与打印机制造商联系以获得合适的打印驱动程序。

文件服务器

您是否计划运行基于域的 Dfs？是 ☐ 否 ☐

备注 基于域的 Dfs 需要运行 Active Directory。

把服务器排列到组以决定每个组将要使用哪一个文件共享：

组_____ 包括以下文件服务器：

_____ _____

_____ _____

_____ _____

_____ _____

_____ _____

应用程序服务器

该应用程序服务器将是哪几种服务的主机？

组件服务 ☐ 终端服务 ☐ 数据库 ☐ E-mail ☐

如果需要组件服务，选择下列项中的一个或多个：

- 应用程序负载平衡：是 ☐ 否 ☐
- 事务服务：是 ☐ 否 ☐
- 应用程序管理：是 ☐ 否 ☐
- 消息队列：是 ☐ 否 ☐
- 其他： _____

_____

Web 服务器

在该服务器上您将安装什么新的或附加组件？

_____

_____

计划升级或全新安装

先导测试是反复的。在受控环境中部署有限数量的计算机，评估测试结果，解决出现的问题，然后部署下一个先导测试直到您的设计达到符合全面部署的范围和质量为止。

为部署确定每个成员服务器的优先次序

为升级或安装创建自己的优先级系统，允许为阶段部署对服务器进行分组。您可能想为每一个先导测试分配一个组号或名称，这有助于稍后确定升级或安装服务器的优先顺序。

先导测试组号或名称是： _____

计划何时在该特定服务器上进行升级或全新安装？选择下列中的一个：

先导测试阶段 1 □ 先导测试阶段 2 □ 生产 □

关于下列项的详细信息：

- 建立测试实验室，请参见本书中的“建立 Windows 2000 测试实验室”。
- 创建先导测试规划，请参见本书中的“实施 Windows 2000 先导测试”。

确保应用程序和服务的可用性

为了创建使应用程序和服务高度可用的规划，对于每一个希望在本单位高度可用的关键任务应用程序或服务，填写一个群集部署规划表。

在开始填写这些表之前，请参见“确保应用程序和服务的可用性”。本章将介绍新概念并提供所需的指导以帮助您最大程度地利用规划表。

明确高可用性需求

您的环境可能包含一个或多个下列应用程序或服务的类型：

- 数据库（Microsoft SQL Server 或其它数据库应用程序）
- 群件（Microsoft Exchange Server 或其它群件应用程序）
- Web 服务（Microsoft Internet 信息服务或其他 Web 服务）
- Windows Internet 命名服务 (WINS)
- 动态主机配置协议 (DHCP)
- 内部开发的业务线应用程序
- 第三方应用程序

- 文件和打印共享

在下面的子部分中为每一个关键任务应用程序或服务定义规范，这些应用程序或服务是您希望部署与 Windows 2000 Server 共同使用的。

应用程序和服务规范

应用程序或服务名称： _____

此应用程序或服务的高可用性要求

该应用程序或服务需要哪一个网络协议？

TCP/IP ☐ IPX/SPX ☐

备注 Microsoft 不提供支持 IPX/SPX 的高可用性解决方案。

您的群集解决方案是否需要以下部分？

提供数据备份 ☐
保护对数据的访问 ☐
保护数据本身 ☐
电力中断时的保护 ☐
网络中断时的保护 ☐
管理群集对象和配置 ☐
与群集中的群集服务的其它实例协调 ☐
执行故障转移操作 ☐
处理事件通知 ☐
促进其它软件组件之间的通信。 ☐

软件兼容问题：

是否有一个资源 DLL？是 ☐ 否 ☐
是否可能使用一般资源 DLL？是 ☐ 否 ☐
资源 DLL 是否支持：
两节点群集 ☐ N-节点群集 ☐
应用程序安装是否支持：
两节点群集 ☐ N-节点群集 ☐
在 Windows 2000 上应用程序功能是否正确？
是 ☐ 否 ☐
应用程序是否无状态或它是否保持一个客户端状态？
_____

特殊的硬件要求：

系统是否在群集硬件兼容性列表 (HCL) 中?
是 ☐ 否 ☐
系统是否支持大内存？是 ☐ 否 ☐
是否安装 Microsoft Windows 2000 Advanced Server 到任何有超过 4 GB 随机访问存储器 (RAM) 的基于 Intel PAE 的计算机系统？是 ☐ 否 ☐
如果是，需要：

- 检查 HCL 以保证系统和组件支持大内存。
- 使系统和组件互兼容。
- 为系统做一个彻底的备份。
- 修改 boot.ini 文件以包含 PAE 交换。

- 测试系统以保证其工作正常。

  系统将使用：

  SCSI （双节点） ☐ SCSI 交换（N-节点） ☐ 光纤信道（ N-节点） ☐

  环境中有什么网络适配器？

  以太网 ☐ 令牌环 ☐ FDDI ☐ ATM ☐

  其他 _____

  网卡是否列在 HCL 中？是 ☐ 否 ☐

  数据量： _____

  用户数量： _____

  操作时间： _____

此应用程序或服务的大小和性能的期望更改

季节性或其它计划的峰值负载： _____

_____

用户的预期增长率： _____

_____

数据的预期增长率： _____

_____

此应用程序或服务的数据备份和灾难恢复规划

最大故障允许： _____

_____

停机时间造成的影响（选择适用项）：

销售额损失 ☐
生产力降低 ☐
顾客满意度降低 ☐
未履行合同义务或法律责任 ☐
竞争力丧失 ☐
修补时间引起的增加的费用 ☐
其他： _____
_____
_____

停机造成的可测算损失（针对每个应用程序和服务故障，定义超过指定最大容许值的费用）：

_____

_____

站点灾难

是否需要不在现场的功能？是 ☐ 否 ☐

标识单点故障：

网络集线器 ☐
网络路由器 ☐
停电 ☐
服务器连接磁盘 ☐
其它服务器硬件如 CPU 或内存 ☐
服务器软件 ☐
WAN 链接如路由器和专线 ☐
拨号连接 ☐
其他： _____
_____

如果一个应用程序或服务失败，保证可用性的计划是什么？：

_____

_____

如果发生了一个服务失败或故障，您是否有：

RAID：
等级 0（带区） ☐
等级 1（镜像） ☐
等级 5（带有奇偶校验的带区） ☐
备用 SCSI 或光纤信道控制器 是 ☐ 否 ☐
替换磁盘 是 ☐ 否 ☐
针对单个用户的不间断电源供应系统 (UPS) 保护
是 ☐ 否 ☐
针对网络的 UPS 保护（包括集线器、网桥、路由器等）
是 ☐ 否 ☐

使用该清单来开始您的群集备份和恢复策略：

将注册表项映射到每一个资源。 ☐
创建一个编录来记录每一次备份。 ☐
确定一个安全的位置来存放备份。 ☐
使用备份功能创建一张紧急修复软盘。 ☐

规划网络负载平衡

应用程序或服务是否运行在群集内的所有主机上还是每一个主机有其自己的应用程序或服务？

应用程序或服务运行在一个主机上 ☐
所有主机共享一个应用程序或服务 ☐

您的应用程序是否使用 TCP 或 UDP 端口？TCP 端口 ☐ UDP 端口 ☐

群集中主机的数量（ 1-32 ）： _____

备注 一定要确保有足够的多余服务器容量，这样如果一台服务器发生故障，其余服务器能够适应负载的增加。

当使用路由器时，运行模式是什么？单播 ☐ 多播 ☐

为网络负载平衡作特别选择

是否在 TCP/IP 上运行下列各项？

分布式组件对象模型（DCOM）☐
命名管道 ☐
远程过程调用 ☐

选择服务器角色

希望群集中的节点是：

成员服务器 ☐ 域控制器 ☐ 全局编录 ☐

备注 如果选择域控制器，请确定有硬件支持。有关详细信息，请参见本书的“确保应用程序和服务的可用性”。

选择群集模式

是否运行了一个：

单节点群集（故障转移不可用） ☐
具有专用辅助节点的群集 ☐
高可用性配置（使用虚拟服务器的资源可用性）：
单一应用程序类型群集 ☐
多应用程序群集 ☐
复杂混合配置 ☐

规划资源组

该群集需要何种类型的资源？

IP 地址 ☐
网络名称 ☐
物理磁盘 ☐
一般或用户应用程序或服务 ☐
指定： _____

列出每一个资源组内所有基于服务器的应用程序；

_____

_____

环境内将运行多少虚拟服务器？ _____

将运行其他哪些独立于这些组的软件？

_____

_____

在网络环境中哪些硬件、连接和操作系统软件可以受到服务器群集的保护？列出所有非应用程序资源。

_____

_____

列出每个资源的所有依赖关系（包括支持核心资源的所有资源）：

_____

_____

_____

每个资源要求什么故障转移策略？

_____

_____

当做分组决定时，创建管理方便。例如：

- 将文件共享资源和打印后台处理资源集中到一个组。
- 将依赖于某个特定资源的应用程序集中到一个组。

同步 Active Directory 与 Exchange Server 目录服务

“同步 Active Directory 与 Exchange Server 目录服务”一章提供目录同步概念和过程，这些将有助于决定最节省开支又行之有效的方式来集成 Active Directory 和 Microsoft Exchange Server 5.5 版目录服务。

为了创建连接协议规划，您应该为单位需要的每一个连接协议填写一个规划工作表。在工作表中记录连接协议之后，可以开始在 Windows 2000 中配置它们。（见随后的“建立连接协议”）

建立连接协议

连接协议参考号或名称： _____

_____

负责该连接协议的管理员： _____

_____

从哪个目录服务管理对象：

Windows 2000 Active Directory ☐ Exchange Server 5.5 目录服务 ☐

方向：单向 ☐ 双向 ☐

确定连接协议源和目标服务器

单向连接协议：

如果源服务器是一个 Exchange 5.5 服务器：

桥头服务器 ☐ 其他 ☐_____

源服务器名称： _____

如果目标服务器是一个 Windows 2000 服务器：

全局编录 ☐ 域控制器 ☐ 桥头服务器 ☐

目标服务器名称： _____

双向连接协议：

如果第一个源服务器是 Exchange 5.5 服务器：

桥头服务器 □其他 □_____

源服务器名称： _____

如果第一个目标服务器是 Windows 2000 服务器：

全局编录 □ 域控制器 □ 桥头服务器 □

目标服务器名称： _____

如果第二个源服务器是 Windows 2000 服务器：

全局编录 □ 域控制器 □ 桥头服务器 □

源服务器名称： _____

如果第二个目标服务器是一个 Exchange 5.5 服务器：

桥头服务器 □ 其他 □_____

目标服务器名称： _____

使用表 A.18 来确定需要映射的对象。

表 A.18 确定映射的目录对象

Exchange Server 5.5 目录	Active Directory

使用表 A.19 来列出不映射的属性。

表 A.19 列出不映射的属性

Exchange Server 5.5 目录	Active Directory

确定第三方电子邮件同步需求： _____

_____

建立目录同步日程安排

要为您单位创建一个同步日程安排，请参考本书的“同步 Active Directory 与 Exchange Server 目录服务”一章中的目录同步日程安排示例。使用表 A.20 来创建您的目录同步计划。

表 A.20 完成您的目录同步矩阵

小时	星期天	星期一	星期二	星期三	星期四	星期五	星期六
0-1							
1-2							
2-3							
3-4							
4-5							
5-6							
6-7							
7-8							
8-9							
9-10							
10-11							
11-12							
12-13							
13-14							
14-15							
15-16							
16-17							
17-18							
18-19							
19-20							
20-21							
21-22							
22-23							
23-24							

记录目录同步的联系人

架构管理员组

主联系人姓名和电话： _____

_____

辅助联系人姓名和电话： _____

_____

为可能的架构修改预留的时间： _____

Windows 2000 域管理

负责 Window 2000 域的单位： _____

_____

主联系人姓名和电话： _____

_____

辅助联系人姓名和电话： _____

_____

Exchange Server 5.5 站点管理

负责 Exchange 站点的单位： _____

_____

主联系人姓名和电话： _____

_____

辅助联系人姓名和电话： _____

_____

使用该连接协议的理由： _____

_____

_____

测试应用程序与 Windows 2000 的兼容性

许多大型的组织有数百或甚至数千个应用程序。如果您的单位是这种情况，编辑应用程序列表可能非常费时。

您可能需要对每一个应用程序编辑下列信息：

- 应用程序名称和版本。
- 供应商名称。
- 当前状态（例如，在生产中、在开发中、或是不再使用）。
- 用户数目及其业务部门。
- 对您单位的优先级或重要性。
- 使用应用程序所在的当前操作系统。

  包括应用程序是基于客户机还是基于服务器，以及哪些组件驻留在客户机和服务器中。

- Web 应用程序的 Web 站点地址 (URL)。
- 安装要求（例如，安全设置和安装目录）。
- 开发工具或技术（如果是内部开发的）。
- 联系人名称和电话号码（内部的和供应商的）。

如果发现同一供应商有多个联系人，尽可能进行合并。

如果您的一个目标是加强应用程序或更好地规划测试工作，可以通过使用表 A.21 来确定应用程序的优先级。

表 A.21 区分应用程序的优先级

应用程序	应用程序对单位的重要性	用户数量	是否是最新版本？	是否使用或需要本地化版本？
			是 ☐ 否 ☐	是 ☐ 否 ☐
			是 ☐ 否 ☐	是 ☐ 否 ☐
			是 ☐ 否 ☐	是 ☐ 否 ☐
			是 ☐ 否 ☐	是 ☐ 否 ☐
			是 ☐ 否 ☐	是 ☐ 否 ☐
			是 ☐ 否 ☐	是 ☐ 否 ☐
			是 ☐ 否 ☐	是 ☐ 否 ☐
			是 ☐ 否 ☐	是 ☐ 否 ☐

可以使用表 A.22 包含的一系列测试来开始规划一个测试策略。使用适合您单位的其他问题来扩展该列表。为了跟踪测试结果，在表中记录测试是否通过、失败、正在进行或未知。您可能还想包括负责测试应用程序的人的姓名和测试完成或预计完成的时间。

表 A.22 规划和跟踪测试策略

测试	测试负责人	计划测试时间	测试结果	完成日期
全新安装				
升级安装				
卸载				
安装选项				
基本功能和一般任务和步骤				
工作时打开多个应用程序				
使用附加硬件（如扫描仪）工作				
打印				
访问和操作服务器数据				

定义客户管理与配置标准

本书中的“ 定义客户管理与配置标准 ”一章描述了主要的规划步骤，您需要完成这些以满足和管理本单位用户的需要。为此应从理解用户的特殊需求，以及为满足客户，客户服务小组必须定位的问题做起。

表 A.23 帮助确定本单位内不同类型用户的计算需求。根据用户的工作类型（漫游、静止专业、基于任务等）及其在本单位的合适位置（位置和工作组），使用该表对用户分组，并由此为应用程序、配置和自主性开发一般标准。有关随后的一个示例表和那些可以帮助您完成类似表格的信息，请参见本书中的“ 定义客户管理与配置标准 ”。

表 A.23 确定用户的计算需求

	职务 1	职务 2	职务 3
类别			
工作组			
位置			

应用程序要求			
操作系统要求			
计算机硬件要求			
支持要求			
允许的和需要的自主性			

表 A.24 帮助定义主要的客户支持问题并分配人员去解决。在规划的稍后阶段中，您可以使用该表来跟踪解决这些客户支持问题的进度。

表 A.24 定义客户支持问题

支持问题	严重性／频率	所有人	解决方案

如果您希望重新分配客户支持任务，使用表 A.25 定义本单位内这些任务目前在哪里执行和期望在哪里执行。

表 A.25 分配客户管理和支持任务

客户支持任务	目前所有人	建议所有人

定义组策略要求

为了实现您的客户管理标准，需要创建组策略对象，它包括在一系列不同区域内的设置：安全、应用程序、计算机系统、用户环境和特定应用程序。这些选项中的绝大多数在“定义客户管理与配置标准”一章中都有解释。安全问题可以参见“规划分布式安全”一章。（如果计划实施“应用更改与配置管理”一章中描述的功能，可能还需要创建其他设置）。

为了定义本单位的组策略需求，首先应确定所需的策略设置类型。一般将其分为以下部分：

安全设置： _____

_____

将要部署的应用程序包： _____

_____

计算机系统设置： _____

_____

用户环境设置： _____

_____

特定应用程序设置： _____

_____

然后，使用类似 A.26 的表格来决定目录内的对象类型（用户、计算机等），这些对象将应用这些设置：

- 域（密码或帐户策略）
- 客户计算机
- 用户
- 域控制器
- 服务器（应用程序、文件和打印）

在此阶段，您创建的文档应当是组策略结构的第一个草稿。很有可能组策略设置的许多项对本单位内的所有客户计算机、用户、服务器等都是相同的。可以合并这些通用组策略设置到一个针对客户、用户、服务器等的单个组策略对象。

表 A.26 定义 Windows 2000 组策略需求

	域	**客户计算机**	**用户**	**域控制器**	**服务器**
安全性	密码；帐户；Kerberos 策略；PK 信任列表	用户权限； 文件和注册表 ACL； 审核和事件日志； 本地设置	EFS 策略	用户权限； 文件和注册表 ACL； 审核和事件日志； 本地设置	用户权限； 文件和注册表 ACL； 审核和事件日志； 本地设置
应用程序部署		强制核心应用程序	已发行的可选的应用程序和组件	管理工具	管理工具
计算机（硬件）设置		启动脚本； 登录； 磁盘配额； 脱机文件		磁盘配额	移动打印机
用户设置			登录脚本； Internet Explorer 设置； 远程访问； 文件夹重定向； 桌面锁闭； 网络；	禁用标准用户桌面设置	禁用标准用户桌面设置

			系统		
应用程序设置			Office 2000；内部应用程序		

有些组策略设置不能适用于一个特定类型的所有对象。要处理这些单独需求，您可以创建另外的组策略对象或使用“ 定义客户管理与配置标准 ”一章中描述的某些特殊组策略实施选项。比如说，您可能需要一个单独的组策略对象来合理配置那些从远程计算机访问网络的用户的计算机。或者，对于具有管理责任的用户，您可能不希望当他们登录到一个服务器控制台时安装他们的应用程序。对希望保护的系统设置一个“ 环回 ”策略，可以通过补充或替代普通用户设置来防止这种情况发生。

本书中的“ 定义客户管理与配置标准 ”一章将解释许多组策略选项，可以使用它们来自定义和有效地管理组策略。表 A.27 说明可以如何记录组策略的范围和例外情况。

表 A.27 定义组策略的范围和例外情况

组策略设置	范围	例外情况
域（安全）		
工作站（安全、应用程序和系统）		
用户（安全、应用程序和系统）		
域控制器（安全、应用程序和系统）		
服务器（安全、应用程序和系统）		

应用更改与配置管理

本书中的“ 定义客户管理与配置标准 ”一章将要求您针对不同类型的用户定义计算机配置和应用程序需求。通过执行“ 应用更改与配置管理 ”一章中描述的规划步骤，可以使用 Windows 2000 IntelliMirror 和远程 OS 安装来实现新的管理和配置标准。

通过使用 Windows 2000 软件安装和维护功能部署的应用程序可以被发布、分配给用户或分配给计算机。为了理解每一个选项的含义和将其应用于单位的应用程序，请参见本书中的"应用更改与配置管理 ”一章。

使用表 A.28 来记录单位使用的应用程序和您将如何部署它们。

表 A.28 记录应用程序及其管理选项

应用程序	分配给用户	分配给计算机	已发布
	是 ☐ 否 ☐	是 ☐ 否 ☐	是 ☐ 否 ☐
	是 ☐ 否 ☐	是 ☐ 否 ☐	是 ☐ 否 ☐
	是 ☐ 否 ☐	是 ☐ 否 ☐	是 ☐ 否 ☐
	是 ☐ 否 ☐	是 ☐ 否 ☐	是 ☐ 否 ☐
	是 ☐ 否 ☐	是 ☐ 否 ☐	是 ☐ 否 ☐

	是 □ 否 □	是 □ 否 □	是 □ 否 □
	是 □ 否 □	是 □ 否 □	是 □ 否 □

使用表 A.29 来定义单位内的每种类型的用户所适用的更改和配置管理功能。在左边一栏中输入在表 A.23 中定义的用户类型。已完成的表格的外观示例，请参见本书中的“ 应用更改与配置管理 ”。

表 A.29 为用户定义配置管理策略

用户类型	用户数据管理	用户设置管理	软件安装和维护	远程 OS 安装

客户自动安装与升级

在进行 Windows 2000 Professional 的自动安装之前，必须确定该安装是对 Windows 2000 之前的操作系统的升级还是一个全新安装。以下问题可以帮助确定进行升级还是进行全新安装。

1. 您的单位是否正在使用 Windows NT 的管理安装？是 □ 否 □
2. 是否计划使用现有的硬件和软件应用程序？是 □ 否 □

   如果对问题 1 和 2 的回答为是，推荐的方式为升级。

3. 是否计划在新的硬件上安装 Windows 2000？是 □ 否 □
4. 是否计划安装新的为 Windows 2000 环境编写的应用程序？是 □ 否 □

   如果对问题 3 和 4 的回答为是，推荐的方式为全新安装。

使用表 A.30 来记录将使用哪一种自动安装方法和在单位的什么位置使用它们。

表 A.30 记录自动安装方法

方法	使用时间	使用该方法？	何处
Syspart	对拥有不同的硬件的计算机的全新安装使用 Syspart。		
Sysprep	当主控计算机和目标计算机有相同硬件（包括 HAL 和海量存储器）时使用 Sysprep。		
Systems Management Server (SMS)	使用 SMS 对多个系统（特别是地理位置分散时）执行 Windows 2000 Server 的管理升级。		
可引导 CD	在基本输入/输出系统（BIOS）允许从 CD 启动的计算机上，使用可引导 CD 的方法。		
远程 OS	使用远程 OS 安装方式，向所支持的计		

安装	算机远程安装 Windows 2000 Professional 的映像，可以免除物理地访问每台计算机来执行安装的必要。		

使用表 A.31 来记录完成每一个客户安装任务的日期。

表 A.31 记录客户安装任务

任务	完成日期
解决关键规划问题	
创建分发文件夹。	
检查应答文件。	
检查 Windows 2000 安装命令。	
基于关键规划选择应用程序安装方法。	
基于关键规划选择操作系统安装方法。	

附录 B - 安装命令

使用安装命令（Winnt.exe 或 Winnt32.exe）安装 Microsoft® Windows® 2000。本附录提供上述程序文件的命令语法和参数的信息。

本附录内容

使用安装命令安装 Windows 2000

Resource Kit (资源工具包)中的相关信息

- 有关 Windows 2000 自动安装的详细信息，参见本书的“服务器自动安装与升级”。
- 关于应答文件的详细信息，请参阅本书附录 C“无人参与安装的应答文件示例”。

使用安装命令安装 Windows 2000

要安装 Windows 2000，使用适当的 Windows 2000 安装命令：

Winnt32.exe 用于新安装或给运行 Microsoft® Windows NT® version 4.0, Microsoft® Windows® 95 或 Microsoft® Windows® 98 的计算机升级。

Winnt.exe 用于运行 Microsoft® MS-DOS® 或 Microsoft® Windows® 3.*x* 的计算机的新安装（不支持这些操作系统升级）。

这两个命令的选项不同。以下部分是对每个命令的说明。

注意 升级至 Windows 2000 操作系统前，如果您刚升级了任何应用程序，一定要重新启动计算机。

Winnt32.exe 命令语法

Winnt32
[/**checkupgradeonly**]
[/**cmd:***command_line*]
[/**cmdcons**]
[/**copydir:***folder_name*]
[/**copysource:***folder_name*]
[/**debug**[*level*][**:***file_name*]]
[/**m:***folder_name*]
[/**makelocalsource**]
[/**noreboot**]
[/**s:***sourcepath*]
[/**syspart:***drive_letter*]
[/**tempdrive:***drive_letter*]
[/**udf:***ID*[,*UDB_file*]]
[/**unattend**]
[/**unattend**[*seconds*][**:***answer_file*]]

/checkupgradeonly

检查当前操作系统升级与 Windows 2000 的兼容性。这只是一个验证，并不安装 Windows 2000。

/cmd:*command_line*

指定安装程序的图形用户界面 (GUI) 部分完成后执行的命令。在安装结束前，安装程序重新启动计算机并收集必要的配置信息后，这个命令会执行。例如，这个选项可以运行 Cmdlines.txt，Cmdlines.txt 通常指定安装程序结束后立即安装的应用程序。

/cmdcons

为修复失败安装添加恢复控制台选项。

/copydir:*folder_name*

在包含 Windows 2000 文件的文件夹内创建一个子文件夹。例如，如果源文件夹包含一个 Private_drivers 文件夹，该文件夹内有针对对站点的修改，可键入 **/copydir:private_drivers**，把这个文件夹复制到 Windows 2000 文件夹。可以多次使用 **/copydir** 选项。

/copysource:*folder_name*

在包含 Windows 2000 文件的文件夹内临时创建子文件夹。例如，如果源文件夹包含 Private_drivers 文件夹，该文件夹内有对站点的修改，可键入 **/copydir:private_drivers**，让安装程序把这个文件夹复制到 Windows 2000 文件夹并在安装过程中使用它的文件。与 **/copydir** 选项不同，使用 **/copysource** 创建的文件夹在安装结束时删除。

/debug[*level*][*:file_name*]

以规定等级创建调试日志。使用默认设置时，程序创建警告级别为 2 的日志文件 (*%windir%*\Winnt32.log)。日志文件的警告级别如下：0 = 严重错误，1 = 错误，2 = 警告，3 = 信息，4 = 调试的详细信息。每个级别还包含在它之下的级别。

/m:*folder_name*

命令安装程序从备用位置复制替换文件。它命令安装程序先查看备用位置，从这个位置（如果已有文件）而不是从默认位置复制文件。

/makelocalsource

命令安装程序把所有安装源文件复制到本地硬盘。如果从 CD 开始安装而在以后的安装中 CD 不可用，使用 /makelocalsource 获取安装文件。

/noreboot

命令安装程序在 Winn32 的文件复制阶段结束后不要重新启动计算机，这样可以执行其它命令。

/s:*sourcepath*

指定 Windows 2000 文件源位置。默认值是当前文件夹。若要同时从多个服务器复制文件，最多可以指定八个源位置。例如：

```
winnt32 /s:server1 U /s:server8
```

Windows 2000 可以使用多达八个 /S 切换指向其它分布式服务器作为源位置，以便安装到目标计算机上。这种功能可以帮助加快目标计算机安装的文件复制阶段，同时为可以运行安装程序的分布式服务器提供更好的负载平衡能力。例如：

```
path to distribution folder 1\winnt32 [/unattend] [:path\answer.txt]
[/s:path to distribution folder 2] [/s:path to distribution folder 3]
[/s:path to distribution folder 4]
```

/syspart:*drive_letter*

规定可以把安装程序启动文件复制到硬盘，把该硬盘标记为活动，并安装在另一台计算机上。当您启动计算机时，安装程序自动从下一阶段开始。使用这个切换时记住以下几点：

- /syspart 选项必须始终与 /tempdrive 选项一起使用。
- /syspart 和 /tempdrive 必须指向次要硬盘的同一分区。
- 必须在次要硬盘的主磁盘分区上安装 Windows 2000。
- /syspart 切换只能在运行 Windows NT 3.51, Windows NT 4.0 或 Windows 2000 的计算机使用，不能在运行 Windows 95 或 Windows 98 操作系统的计算机使用。

/tempdrive:*drive_letter*

指示安装程序把临时文件放在指定分区上，并把 Windows 2000 安装在那个分区上。使用这个切换时记住以下几点：

- /tempdrive 选项必须始终与 /syspart 选项一起使用。
- /tempdrive 和 /syspart 必须指向次要硬盘的同一分区。
- 必须在次要硬盘的主磁盘分区上安装 Windows 2000。

/udf:*ID[,UDB_file]*

指明安装程序使用的标识符 (ID)，规定唯一性数据库文件 (UDB) 如何修改应答文件（参见下面的 **/unattend** 选项）。.udb 文件替代应答文件中的值，标识符确定使用 .udb 文件中的哪些值。例如，**/udf:Roaming_user,Our_company.udb** 替代 **Our_company.udb** 文件中的标识符 **Roaming_user** 的指定设置。如果不指定 .udb 文件，安装程序提示您插入包含 $*Unique*$.udb 的磁盘。

/unattend

使用无人参与安装模式升级以前版本的 Windows。所有用户设置都取自上一个安装，这样安装过程中不需要用户干涉。

重要 使用 /unattend 切换自动安装肯定您已经看过并接受 Windows 2000 最终用户许可协议 (EULA)。在使用这个切换代表非本单位安装 Windows 2000 前，必须确认最终用户（无论是个人还是单独的实体）已经收到、阅读并接受 Windows 2000 EULA 的条款。初始设备制造商不能在卖给最终用户的机器上指定这个关键字。

/unattend[*seconds*][*:answer_file*]

不使用需要用户交互的提示安装 Windows 2000，相反，安装程序从事先准备的应答文件获取需要的信息。关于应答文件的详细信息，参见本书附录 C“无人参与安装的应答文件示例”。

只有从 Windows NT 4.0 升级时包含“*seconds*”。“*seconds*”以秒为单位指定安装程序完成文件复制和系统安装开始之间的延迟。

Winnt.exe 命令语法

Winnt
[**/E:***command*]

[/**R:***folder_name*]
[/**Rx:***folder_name*]
[/**S:***sourcepath*]
[/**T**[**:***tempdrive*]]
[/**U**[**:***answer_file*]]
[/**udf:***ID*[,UDB_file]
[/**A**:]

/E:*command*

指定安装的 GUI 部分完成后执行的命令。例如，这个选项可以运行 Cmdlines.txt，Cmdlines.txt 通常指定安装程序结束后立即安装的应用程序。

/R:*folder_name*

在包含 Windows 2000 文件的文件夹内创建一个子文件夹。例如，如果源文件夹包含一个 Private_drivers 文件夹，该文件夹内有针对站点的修改，可以键入 **/R:private_drivers**，把这个文件夹复制到 Windows 2000 文件夹。可以多次使用 **/R** 选项。

/Rx:*folder_name*

在包含 Windows 2000 文件的文件夹内临时创建子文件夹。例如，如果源文件夹包含一个 Private_drivers 文件夹，该文件夹内有针对站点的修改，可以键入 **/ Rx:private_drivers**，让安装程序把这个文件夹复制到 Windows 2000 文件夹并在安装过程中使用它的文件。与 **/R** 选项不同，使用 **/Rx** 创建的文件夹在安装结束时删除。

/S:*sourcepath*

指定 Windows 2000 文件源位置。该位置必须是 Drive_letter:\Path 或 \\Server\Share\Path 形式的完整路径。默认值是当前文件夹。

/T:*tempdrive*

指示安装程序把临时文件放在指定驱动器上，并把 Windows 2000 安装在那个驱动器上。如果您不指定位置，安装程序会为您找出驱动器。

/U:*answer_file*

不使用需要用户交互的提示安装 Windows 2000，相反，安装程序从事先准备的应答文件获取需要的信息。关于应答文件的详细信息，参见本书附录 C“无人值守安装的应答文件示例”。需要 **/S**。

/udf:ID[,*UDB_file*]

指明安装程序使用的标识符 (ID)，规定唯一性数据库文件 (UDB) 如何修改应答文件。.udb 文件替代应答文件中的值，标识符确定使用 .udb 文件中的哪些值。例如，**/udf:Roaming_user,Our_company.udb** 替代 **Our_company.udb** 文件中的标识符 **Roaming_user** 的指定设置。如果不指定 .udb 文件，安装程序提示您插入包含 $*Unique*$.udb 的磁盘。

/A

启用辅助功能选项。

附录 C - 无人参与安装的应答文件示例

Microsoft® Windows® 2000 无人参与安装使用称为应答文件的 ASCII 文本文件提供数据，否则这些数据就要在您运行安装向导时交互输入。使用无人参与安装选项时，应答文件在 Winnt.exe 或 Winnt32.exe 命令行上指定。（关于何时使用哪个命令行的详细信息，参见本书附录 B“安装命令”。）

本附录包含适合一般安装配置的应答文件示例。可以自定义 Windows 2000 默认应答文件 (Unattend.txt) 或以本附录提供的示例为基础写一个新文件。

本附录内容

在 Resource Kit (资源工具包) 中的相关信息

- 有关安装命令的详细信息，参见本书附录 B“安装命令”。

应答文件格式

应答文件由节标题、关键字和每个关键字的值组成。大多数节标题是预定义的，但有些也可由用户定义。如果安装程序不需要，就不必在应答文件中指定所有可能的关键字。无效关键字值在安装后会产生错误或导致不正确的操作。文件格式如下：

```
[section_name]
```

节包含关键字和这些关键字的相应值。每个关键字和值都由一个空格、一个等号和一个空格隔开。以下是一个示例：

```
key = value
```

中间有空格的值通常需要在两边加双引号。以下是一个示例：

```
key = "value with spaces"
```

有些节没有关键字而只包含一个值的列表。以下是一个示例：

```
[OEMBootFiles]
Txtsetup.oem
```

注释行以分号作为开始。

```
; This is an example of a comment line.
```

应答文件关键字及其值

应答文件中的每个关键字必须有赋给它的值，有些关键字是可选项，有些有默认值，这些默认值在关键字被省略时使用。

关键字的值是文本字符串，除非指定成数字。如果指定成数字，这个值是十进制的，除非另有规定。

备注 关键字不分大小写，既可以大写，也可以小写。

关于应答文件关键字及其值的详细信息，参见 Windows 2000 操作系统 CD 中的《Microsoft Windows 2000 Guide to Unattended Setup》(Unattend.doc)。Unattend.doc 文件是 \Support\Tools 文件夹中 Deploy.cab 文件的一部分。在 Windows 98 或 Windows 2000 中，使用 Windows 资源管理器将这个文档解压缩。在 Windows 的更早版本或 MS-DOS 中，使用 Extract 命令访问该文件。

应答文件示例

本节提供的应答文件示例是一些配置中通常使用的关键字的安装配置的举例。这些文件只是些例子，根据您单位的情况做适当的修改。

备注 在下面的应答文件中，使用斜体字部分表明用户必须提供要求的信息。

同时，为引起每个节的注意，节的名称是粗体字；但是在您的应答文件中不必按照这个格式。

示例 1 — 默认 Unattend.txt

以下应答文件是 Windows 2000 CD 上提供的默认 Unattend.txt 文件。

```
; Microsoft Windows 2000 Professional, Server, Advanced Server
; © 1994–1999 Microsoft Corporation.All rights reserved.
;
; Sample Answer File for Unattended Setup
;
; This file contains information about how to automate the installation
; or upgrade of Windows 2000 Professional and Windows 2000 Server so
; that the Setup program runs without requiring user input.
;
```

[Unattended]
UnattendMode = FullUnattended
OemPreinstall = No
TargetPath = Winnt
Filesystem = LeaveAlone

[UserData]
FullName = "*Your user name*"
OrgName = "*Your organization name*"
```
; It is recommended that you avoid using spaces in the ComputerName
; value.
```
ComputerName = "*YourComputer_name*"
```
; To ensure a fully unattended installation, you must provide a value
; for the ProductId key.
```
ProductId = "Your product *ID*"

[GuiUnattended]
```
; Sets the TimeZone.For example, to set the TimeZone for the
; Pacific Northwest, use a value of "004."Be sure to use the
; numeric value that represents your own time zone.To look up
; a numeric value, see the Unattend.doc file on the Windows 2000 CD.
```
TimeZone = "*YourTimeZone*"
```
; It is recommended that you change the administrator password
; before the computer is placed at its final destination.
```
AdminPassword = AdminPassword
```
; Tells Unattended Setup to turn AutoLogon on and log on once.
```

```
AutoLogon = Yes
AutoLogonCount = 1

[LicenseFilePrintData]
; This section is used for server installs.
AutoMode = "PerServer"
AutoUsers = "5"

[GuiRunOnce]
; List the programs that you want to start when you log on to the
; computer for the first time.

[Display]
BitsPerPel = 8
XResolution = 800
YResolution = 600
VRefresh = 70

[Networking]
; When you set the value of the InstallDefaultComponents key
; to Yes, Setup will install default networking components.
; The components to be set are TCP/IP, File and Print Sharing,
; and Client for Microsoft Networks.
InstallDefaultComponents = Yes

[Identification]
; Identifies your workgroup. It is recommended that you avoid
; using spaces in this value.
JoinWorkgroup = "YourWorkgroup"
```

示例 2 — 使用 CD-ROM 的 Windows 2000 Professional 的无人参与安装

以下应答文件从 CD-ROM 安装 Microsoft® Windows® 2000 Professional。要让这个应答文件正常工作，必须把它命名为 Winnt.sif 并拷到软盘上。

```
; Microsoft Windows 2000 Professional
; © 1994–1999 Microsoft Corporation.All rights reserved.
;
; Sample Answer File for Unattended Setup
;
; This file contains information about how to automate the installation
; or upgrade of Windows 2000 Professional so that the Setup program runs
; without requiring user input.
;

[Data]
; This section is required when you perform an unattended installation
; by starting Setup directly from the Windows 2000 installation CD-ROM.
Unattendedinstall = Yes
; If you are running Unattended Setup from the CD-ROM, you must set the
; Msdosinitiated key to 0.
Msdosinitiated = "0"
; AutoPartition allows Windows 2000 Unattended Setup to choose a
; partition to install to.
AutoPartition = 1

[Unattended]
```

```
UnattendMode = FullUnattended
; The OemPreinstall key tells Unattended Setup that the installation is
; being performed from distribution shares if the value is set to Yes.
OemPreinstall = Yes
TargetPath = Winpro
FileSystem = LeaveAlone
; If the OemSkipEula key is set to Yes, it informs Unattended Setup that
; the user should not be prompted to accept the End User License
; Agreement (EULA). A value of Yes signifies agreement to the EULA and
; should be used in conjunction with the terms of your license
; agreement.
OemSkipEula = Yes

[GuiUnattended]
; Sets the TimeZone. For example, to set the TimeZone for the
; Pacific Northwest, use a value of "004." Be sure to use the
; numeric value that represents your own time zone. To look up
; a numeric value, see the Unattend.doc file on the Windows 2000 CD.
TimeZone = "YourTimeZone"
; It is recommended that you change the administrator password
; before the computer is placed at its final destination.
AdminPassword = AdminPassword
; Tells Unattended Setup to turn AutoLogon on and log on once.
AutoLogon = Yes
AutoLogonCount = 1
; The OemSkipWelcome key specifies whether the welcome page in the
; wizard phase of Setup should be skipped. A value of 1 causes the page
; to be skipped.
OemSkipWelcome = 1
; The OemSkipRegional key allows Unattended Setup to skip
; RegionalSettings when the final location of the computer is unknown.
OemSkipRegional = 1

[UserData]
FullName = "Your user name"
OrgName = "Your organization name"
; It is recommended that you avoid using spaces in the
; ComputerName value.
ComputerName = "YourComputer_name"
; To ensure a fully unattended installation, you must provide a value
; for the ProductId key.
ProductId = "Your product ID"

[Display]
BitsPerPel = 8
XResolution = 800
YResolution = 600
VRefresh = 60

[Networking]
; When you set the value of the InstallDefaultComponents key
; to Yes, Setup will install default networking components.
; The components to be set are TCP/IP, File and Print Sharing,
; and Client for Microsoft Networks.
InstallDefaultComponents = Yes
```

示例 3 — 安装和配置 Windows 2000 并配置 Microsoft Internet Explorer 的代理设置

以下应答文件安装和配置 Microsoft® Internet Explorer，配置代理设置。

```
; Microsoft Windows 2000 Professional, Server, Advanced Server
; © 1994–1999 Microsoft Corporation. All rights reserved.
;
; Sample Answer File for Unattended Setup
;
; This file contains information about how to automate the installation
; or upgrade of Windows 2000 Professional and Windows 2000 Server so
; that the Setup program runs without requiring user input.
;
```

[Unattended]
UnattendMode = FullUnattended
TargetPath = Windows
FileSystem = LeaveAlone
OemPreinstall = Yes
OemSkipEula = Yes

[GuiUnattended]
```
; Sets the TimeZone. For example, to set the TimeZone for the
; Pacific Northwest, use a value of "004." Be sure to use the
; numeric value that represents your own time zone. To look up
; a numeric value, see the Unattend.doc file on the Windows 2000 CD.
```
TimeZone = "*YourTimeZone*"
```
; It is recommended that you change the administrator password
; before the computer is placed at its final destination.
```
AdminPassword = AdminPassword
```
; Tells Unattended Setup to turn AutoLogon on and log on once.
```
AutoLogon = Yes
AutoLogonCount = 1
OemSkipWelcome = 1
```
; The OemSkipRegional key allows Unattended Setup to skip
; RegionalSettings when the final location of the computer is unknown.
```
OemSkipRegional = 1

[UserData]
FullName = "*Your user name*"
OrgName = "*Your organization name*"
; It is recommended that you avoid using spaces in the
; ComputerName value.
ComputerName = "*YourComputername*"
```
; To ensure a fully unattended installation, you must provide a value
; for the ProductId key.
```
ProductId = "*Your product ID*"
[LicenseFilePrintData]
```
; This section is used for server installs.
```
AutoMode = "PerServer"
AutoUsers = "50"

[Display]
BitsPerPel = 8
XResolution = 800
YResolution = 600

```
VRefresh = 60

[Components]
; This section contains keys for installing the components of
; Windows 2000. A value of On installs the components, and a
; value of Off prevents the component from being installed.
iis_common = On
iis_inetmgr = Off
iis_www = Off
iis_ftp = Off
iis_htmla = Off
iis_doc = Off
iis_pwmgr = Off
iis_smtp = On
iis_smtp_docs = Off
Mts_core = On
; The Fp key installs Front Page Server Extensions.
Fp = On
Msmq = Off
; If you set the TSEnable key to On, Terminal Services is installed on
; Windows 2000 Server.
TSEnable = On
; If you set the TSClients key to On, the files required to create
; Terminal Services client disks are installed. If you set this key
; to On, you must also set the TSEnable key to On.
TSClients = On
; TSPrinterDrivers and TSKeyboardDrivers are optional keys. If enabled,
; they require additional disk space.
TSPrinterDrivers = Off
TSKeyboardDrivers = Off
Netoc = On
Reminst = On
Certsrv = Off
Rstorage = Off
Indexsrv_system = On
Certsrv_client = Off
Certsrv_server = Off
Certsrv_doc = Off
Accessopt = On
Calc = On
Cdplayer = On
Charmap = On
Chat = Off
Clipbook = On
Deskpaper = On
Dialer = On
Freecell = Off
Hypertrm = On
Media_blindnoisy = On
Media_blindquiet = On
Media_clips = On
Media_jungle = On
Media_musica = On
Media_robotz = On
Media_utopia = On
Minesweeper = Off
Mousepoint = Off
Mplay = On
```

Mswordpad = On
Objectpkg = On
Paint = On
Pinball = Off
Rec = On
Solitaire = Off
Templates = On
Vol = On

[TapiLocation]
CountryCode = "1"
Dialing = Pulse
; Indicates the area code for your telephone. This value should
; be a 3-digit number.
AreaCode = "Your telephone area code"
LongDistanceAccess = 9

[Networking]
; When you set the value of the InstallDefaultComponents key
; to Yes, Setup will install default networking components.
; The components to be set are TCP/IP, File and Print Sharing,
; and Client for Microsoft Networks.
InstallDefaultComponents = Yes

[Identification]
JoinDomain = *YourCorpNet*
DomainAdmin = *YourCorpAdmin*
DomainAdminPassword = *YourAdminPassword*

[NetOptionalComponents]
; This section contains a list of the optional network
; components to install.
Wins = Off
Dns = Off
Dhcpserver = Off
ils = Off
Snmp = Off
Lpdsvc = Off
Simptcp = Off
Netmontools = On
Dsmigrat = Off

[Branding]
; This section brands Microsoft Internet Explorer with custom
; properties from the Unattended answer file.
BrandIEUsingUnattended = Yes

[URL]
; This section contains custom URL settings for Microsoft
; Internet Explorer. If these settings are not present, the
; default settings are used. Specifies the URL for the
; browser's default home page. For example, you might use the
; following: Home_Page = www.microsoft.com.
Home_Page = *YourHomePageURL*
; Specifies the URL for the default search page. For example, you might
; use the following: Search Page = www.msn.com
Search_Page = *YourSearchPageURL*
; Specifies a shortcut name in the link folder of Favorites.
; For example, you might use the following: Quick_Link_1_Name =
; "Microsoft Product Support Services"

Quick_Link_1_Name = "*Your Quick Link Name*"
; Specifies a shortcut URL in the link folder of Favorites. For example,
; you might use this: Quick_Link_1 = http://support.microsoft.com/.
Quick_Link_1 = *YourQuickLinkURL*

[Proxy]
; This section contains custom proxy settings for Microsoft
; Internet Explorer. If these settings are not present, the default
; settings are used. If **proxysrv:80** is not accurate for your
; configuration, be sure to replace the proxy server and port number
; with your own parameters.
HTTP_Proxy_Server = *proxysrv:80*
Use_Same_Proxy = 1
Proxy_Enable = 1
Proxy_Override = <local>

示例 4 — 安装和配置带两个网卡的 Windows 2000 Server

以下应答文件安装带两个网卡的 Microsoft® Windows® 2000 Server；一个网卡使用动态主机配置协议 (DHCP)，另一个使用静态信息。

; Microsoft Windows 2000 Server, Advanced Server
; © 1994–1999 Microsoft Corporation. All rights reserved.
;
; Sample Answer File for Unattended Setup
;
; This file contains information about how to automate the installation
; or upgrade of Windows 2000 Server or Windows 2000 Advanced Server so
; that the Setup program runs without requiring user input.
;

[Unattended]
UnattendMode = FullUnattended
TargetPath = Winnt
Filesystem = ConvertNTFS

[GuiUnattended]
; Sets the TimeZone. For example, to set the TimeZone for the
; Pacific Northwest, use a value of "004." Be sure to use the
; numeric value that represents your own time zone. To look up
; a numeric value, see the Unattend.doc file on the Windows 2000 CD.
TimeZone = "*YourTimeZone*"
; It is recommended that you change the administrator password
; before the computer is placed at its final destination.
AdminPassword = AdminPassword
; Tells Unattended Setup to turn AutoLogon on and log on once.
AutoLogon = Yes
AutoLogonCount = 1

[LicenseFilePrintData]
; This section is used for server installs.
AutoMode = "PerServer"
AutoUsers = "50"

[UserData]
FullName = "*Your user name*"
OrgName = "*Your organization name*"
; It is recommended that you avoid the use of spaces in the
; ComputerName value.

ComputerName = "*YourComputer_name*"
; To ensure a fully unattended installation, you must provide a value
; for the ProductId key.
ProductId = "*Your product ID*"

[Display]
BitsPerPel = 8
XResolution = 800
YResolution = 600
VRefresh = 70

[Networking]
; When you set the value of the InstallDefaultComponents key
; to Yes, Setup will install default networking components.
; The components to be set are TCP/IP, File and Print Sharing,
; and Client for Microsoft Networks.
InstallDefaultComponents = Yes

[Identification]
JoinDomain = *YourCorpNet*
DomainAdmin = *YourCorpAdmin*
DomainAdminPassword = *YourAdminPassword*

[NetAdapters]
; In this example, there are two network adapters, Adapter01
; and Adapter02. Note that the adapter specified here as 01 is not
; always local area network (LAN) connection 1 in the user interface.
Adapter01 = Params.Adapter01
Adapter02 = Params.Adapter02

[Params.Adapter01]
; Specifies which adapter is number one. Note that the InfID key
; must match a valid PNP ID in the system. For example, a valid
; PNP ID might look like the following: InfID = "pci\ven_0e11&dev_ae32"
InfID = "*Your_PNP_ID_for_Adapter01*"

[Params.Adapter02]
; Specifies which adapter is number two. Note that the InfID key must
; match a valid PNP ID in the system. For example, a valid PNP ID
; might look as follows: InfID = "pci\ven_8086&dev_1229&subsys_00018086"
InfID = " *Your_PNP_ID_for_Adapter02*"

[NetClients]
; Installs the Client for Microsoft Networks.
MS_MSClient = params.MS_MSClient

[Params.MS_MSClient]

[NetProtocols]
; Installs only the TCP/IP protocol.
MS_TCPIP = params.MS_TCPIP

[params.MS_TCPIP]
; This section configures the TCP/IP properties.
AdapterSections = Params.MS_TCPIP.Adapter01,params.MS_TCPIP.Adapter02

[Params.MS_TCPIP.Adapter01]
; Adapter01 uses DHCP server information.
SpecificTo = Adapter01
DHCP = Yes

Wins = Yes

[Params.MS_TCPIP.Adapter02]
; Adapter02 uses static TCP/IP configuration.
SpecificTo = Adapter02
IPAddress = 1.1.1.1
SubnetMask = 255.255.248.0
DefaultGateway = 2.2.2.2
DHCP = No
Wins = No

[NetServices]
; Install File and Print services.
MS_Server = Params.MS_Server

[Params.MS_Server]

示例 5 — 安装带网络负载平衡的 Windows 2000 Advanced Server

以下应答文件安装带网络负载平衡的 Microsoft® Windows® 2000 Advanced Server。

```
; Microsoft Windows 2000 Advanced Server
; © 1994–1999 Microsoft Corporation. All rights reserved.
;
; Sample Answer File for Unattended Setup
;
; This file contains information about how to automate the installation
; or upgrade of Windows 2000 Advanced Server so that the
; Setup program runs without requiring user input.
;
```

[Unattended]
UnattendMode = FullUnattended
TargetPath = Windows
FileSystem = ConvertNTFS

[GuiUnattended]
; Sets the TimeZone. For example, to set the TimeZone for the
; Pacific Northwest, use a value of "004." Be sure to use the
; numeric value that represents your own time zone. To look up
; a numeric value, see the Unattend.doc file on the Windows 2000 CD.
TimeZone = "*YourTimeZone*"
; It is recommended that you change the administrator password
; before the computer is placed at its final destination.
AdminPassword = AdminPassword
; Tells Unattended Setup to turn AutoLogon on and log on once.
AutoLogon = Yes
AutoLogonCount = 1
AdvServerType = Servernt

[LicenseFilePrintData]
; This section is used for server installs.
AutoMode = "PerServer"
AutoUsers = "50"

[UserData]
FullName = "*Your user name*"

OrgName = "*Your organization name*"
; It is recommended that you avoid the use of spaces in the
; COMPUTERNAME VALUE.
ComputerName = "*YourComputer_name*"
; To ensure a fully unattended installation, you must provide a value
; for the ProductId key.
ProductId = "*Your product ID*"

[Display]
BitsPerPel = 8
XResolution = 800
YResolution = 600
VRefresh = 70

[Networking]
; When you set the value of the InstallDefaultComponents key
; to Yes, Setup will install default networking components.
; The components to be set are TCP/IP, File and Print Sharing,
; and Client for Microsoft Networks.
InstallDefaultComponents=Yes

[Identification]
JoinDomain = *YourCorpNet*
DomainAdmin = *YourCorpAdmin*
DomainAdminPassword = *Your AdminPassword*

[NetAdapters]
; In this example, there are two network adapters, Adapter01
; and Adapter02. Note that the adapter specified here as 01 is not
; always local area network (LAN) connection 1 in the user interface.
; The network adapters in this example are not identical.
Adapter01 = Params.Adapter01
Adapter02 = Params.Adapter02

[NetBindings]
Enable = MS_WLBS, Adapter01
Enable = MS_TCPIP, Adapter02

[Params.Adapter01]
; Specifies which adapter is number one.
PseudoAdapter = No
PreUpgradeInstance = *E100B1*
; Note that the InfID key must match a valid PNP ID in the
; system. For example, a valid PNP ID might look like the
; following: InfID = PCI\VEN_8086&DEV_1229.
InfID = *Your_PNP_ID_for_Adapter01*
BusType = PCI
; The ConnectionName key specifies the name for the network connection
; associated with the network adapter that you are installing.
ConnectionName = "*Connection1*"

[Params.Adapter02]
; Specifies which adapter is number two.
PseudoAdapter = No
PreUpgradeInstance = *El90x2*
; Note that the InfID key must match a valid PNP ID in the
; system. For example, a valid PNP ID might look like the
; following: InfID = *PCI\VEN_10b7&DEV_9050*
InfID = *Your_PNP_ID_for_Adapter02*
BusType = PCI

```
; The ConnectionName key specifies the name for the network connection
; associated with the network adapter that you are installing.
```
ConnectionName = "*Connection2*"

[NetProtocols]
MS_TCPIP = Params.MS_TCPIP
MS_NetMon = Params.MS_NetMon

[Params.MS_TCPIP]
AdapterSections = params.MS_TCPIP.Adapter01,params.MS_TCPIP.Adapter02

[Params.MS_TCPIP.Adapter01]
SpecificTo = Adapter01
DNSServerSearchOrder = 192.31.56.150
Wins = Yes
WinsServerList = 192.31.56.150
NetBIOSOptions = 0
DHCP = No
IPAddress = 192.31.56.90,192.31.56.91
SubnetMask = 255.255.255.0,255.255.255.0
DefaultGateway = 192.31.56.150

[Params.MS_TCPIP.Adapter02]
SpecificTo = Adapter02
DNSServerSearchOrder = 192.31.56.150
Wins = Yes
WinsServerList = 192.31.56.150
NetBIOSOptions = 0
DHCP = No
IPAddress = 192.31.56.92
SubnetMask = 255.255.255.0
DefaultGateway = 192.31.56.150

[Params.MS_NetMon]

[Params.MS_WLBS]
```
; This section contains keys specific to setting the properties of
; Network Load Balancing.
```
HostPriority = 1
ClusterModeOnStart = 0
ClusterIPAddress = 192.31.56.91
ClusterNetworkMask = 255.255.255.0
DedicatedIPAddress = 192.31.56.90
DedicatedNetworkMask = 255.255.255.0
ClusterName = *cluster.domain.com*
MulticastSupportEnable = 0
MaskSourceMAC = 1
RemoteControlCode = 0x00000000
RemoteControlUDPPort = 2504
RemoteControlEnabled = 1
Ports = 80,80,Both,Multiple,None,Equal,443,443,Both,Multiple,Single,Equal
AliveMsgPeriod = 2000
AliveMsgTolerance = 10
NumActions = 50
NumPackets = 100
NumAliveMsgs = 10
DescriptorsPerAlloc = 512

MaxDescriptorAllocs = 512
ConnectionCleanupDelay = 300000
NBTSupportEnable = 1

[NetClients]
MS_MSClient = Params.MS_Client

[Params.MS_Client]

[NetServices]
MS_Server = Params.MS_Server
MS_WLBS = Params.MS_WLBS

[Params.MS_Server]
Optimizations = Balance

[NetOptionalComponents]
Netmontools = 1

示例 6 — 安装带 Windows 群集的 Windows 2000 Advanced Server

以下应答文件安装带 Windows 群集的 Windows 2000 Advanced Server。

```
; Microsoft Windows 2000 Advanced Server.
; © 1994–1999 Microsoft Corporation. All rights reserved.
;
; Sample Answer File for Unattended Setup
;
; This file contains information about how to automate the installation
; or upgrade of Windows 2000 Advanced Server so that the Setup program
; runs without requiring user input.
;
```

[Unattended]
UnattendMode = FullUnattended
TargetPath = Advsrv
FileSystem = ConvertNTFS
OemPreinstall = Yes
OemSkipEula = Yes

[GuiUnattended]
```
; Sets the TimeZone. For example, to set the TimeZone for the
; Pacific Northwest, use a value of "004." Be sure to use the
; numeric value that represents your own time zone. To look up
; a numeric value, see the Unattend.doc file on the Windows 2000 CD.
```
TimeZone = "*YourTimeZone*"
```
; It is recommended that you change the administrator password
; before the computer is placed at its final destination.
```
AdminPassword = AdminPassword
```
; Tells Unattended Setup to turn AutoLogon on and log on once.
```
AutoLogon = Yes
AutoLogonCount = 1
AdvServerType = Servernt
OemSkipWelcome = 1
```
; The OemSkipRegional key allows Unattended Setup to skip
; RegionalSettings when the final location of the computer is unknown.
```

OemSkipRegional = 1

[LicenseFilePrintData]
; This section is used for server installs.
AutoMode = "PerServer"
AutoUsers = "50"

[UserData]
FullName = "*Your user name*"
OrgName = "*Your organization name*"
; It is recommended that you avoid the use of spaces in the
; ComputerName value.
ComputerName = "*YourComputer_name*"
; To ensure a fully unattended installation, you must provide a value
; for the ProductId key.
ProductId = "*Your product ID*"

[Display]
BitsPerPel = 8
XResolution = 800
YResolution = 600
VRefresh = 70

[Networking]
; When you set the value of the InstallDefaultComponents key
; to Yes, Setup will install default networking components.
; The components to be set are TCP/IP, File and Print Sharing,
; and Client for Microsoft Networks.
InstallDefaultComponents = Yes

[Identification]
JoinDomain = *YourCorpNet*
DomainAdmin = *YourCorpAdmin*
DomainAdminPassword = *YourAdminPasswor*d

[NetAdapters]
; In this example there are three network adapters, Adapter 01,
; Adapter 02, and Adapter 03. The adapter specified here as 01 is not
; always LAN connection 1 in the user interface. The network adapters
; in this example are not identical.

Adapter01 = Params.Adapter01
Adapter02 = Params.Adapter02
Adapter03 = Params.Adapter03

[Params.Adapter01]
; Specifies which adapter is number one.
; Note that the NetCardAddress key must match a valid address of the
; adapter in the system. For example, a valid address might look like
; the following: NetCardAddress = 0x00C04F778A5A
NetCardAddress = *YourNetCardAddress*
; The ConnectionName key specifies the name for the network connection
; associated with the network adapter that you are installing.
ConnectionName = *CorpNet*

[Params.Adapter02]
; Specifies which adapter is number two. Note that the
; NetCardAddress key must match a valid address of the adapter
; in the system. For example, a valid address might look like the
; following: NetCardAddress = 0x00C04F778A5A

NetCardAddress = *YourNetCardAddress*
; The ConnectionName key specifies the name for the network connection
; associated with the network adapter that you are installing.
ConnectionName = *VendorNet*

[Params.Adapter03]
; Specifies which adapter is number three. Note that the
; NetCardAddress key must match a valid address of the adapter
; in the system. For example, a valid address might look like the
; following: NetCardAddress = 0x00C04F778A5A
NetCardAddress = *YourNetCardAddress*
; The ConnectionName key specifies the name for the network connection
; associated with the network adapter that you are installing.
ConnectionName = *PrivateNet*

[NetClients]
; Installs the Client for Microsoft Networks.
MS_MSClient = Params.MS_MSClient

[Params.MS_MSClient]

[NetProtocols]
; Installs only the TCP/IP protocol.
MS_TCPIP = Params.MS_TCPIP

[Params.MS_TCPIP]
; This section configures TCP/IP properties.
AdapterSections = Params.MS_TCPIP.Adapter01,params.MS_TCPIP.Adapter02,params.MS_TCPIP.Adapter03

[Params.MS_TCPIP.Adapter01]
; CorpNet on Adapter01 uses DHCP server information.
SpecificTo = Adapter01
DHCP = Yes
DNSServerSearchOrder = 172.31.240.226, 172.31.240.225
DNSSuffixSearchOrder = *CorpNet, dns.domain.com*
DNSDomain = *CorpNet*

[Params.MS_TCPIP.Adapter02]
; VendorNet on Adapter02 uses local DHCP information.
SpecificTo = Adapter02
DHCP = Yes

[Params.MS_TCPIP.Adapter03]
; PrivateNet on Adapter03 uses static information.
SpecificTo = Adapter03
DHCP = No
WINS = No
IPAddress = 10.2.0.41
SubnetMask = 255.255.0.0
DefaultGateway = 2.2.2.2
DNSServerSearchOrder = 10.2.0.253, 10.2.0.254

[NetServices]
; Installs File and Print services.
MS_Server = Params.MS_Server

[Params.MS_Server]

[Components]

```
; Installs Windows Clustering and Administration components on
; Advanced Server when you set the value to On.
```
Cluster = On

[Cluster]
Name = *CorpCluster*
Action = Form
Account = *CorpAdmin*
Domain = *CorpNet*
IPAddr = 172.31.240.227
Subnet = 255.255.248.0
Network = *CorpNet,ALL*
Network = *VendorNet,ALL*

[GuiRunOnce]
```
; You can automate the running of Cluscfg.exe by placing Cluscfg.exe
; in the [GuiRunOnce] section of the Unattended answer file. This
; executes Cluscfg.exe and configures clustering on the first startup
; after GUI mode Setup has completed.
; You must include the full path to the program between the quotes.
```
"%Windir%\Cluster\Cluscfg.exe –unattend"

[NetOptionalComponents]
NETMONTOOLS = 1

附录 D - 部署工具

本书提供了帮助您部署 Microsoft® Windows® 2000 的工具的参考信息。表 D.1 给出了这些工具的摘要信息，让您可以很快了解它们的名称和简短说明。

到哪里查找这些工具的详细信息：

可以在下列位置找到本附录提到的工具的其它信息：

- 有关与 Windows 2000 操作系统一起提供的工具的信息，参见 Windows 2000 帮助。
- 有关安装和使用 Windows 2000 Support Tools 和 Support Tools 帮助的信息，参见 Windows 2000 操作系统 CD 的 \Support\Tools 文件夹中的 Sreadme.doc 文件。
- 有关包含在完整的《Microsoft® Windows® 2000 Server Resource Kit》中的工具的信息，参见 Web 资源页的资源链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources。

备注 工具名称旁边的星号 (*) 代表此工具包含在 Windows 2000 操作系统 CD 上。不是所有这些工具都在安装操作系统时默认安装，有些则作为 Windows 2000 Support Tools 的一部分安装。

表 D.1 部署工具

工具名称	文件名	在本书中的位置	说明
* Active Directory 连接器 (ADC) MMC 管理单元	Adcadmin.msc	第 20 章，“将 Active Directory 与 Exchange Server 目录服务同步”	此 Microsoft® 管理控制台 (MMC) 管理单元让您可以将 Microsoft® Active Directory™ 和 Microsoft® Exchange Server 5.5 版目录服务之间的通信同步并管理通信。
* Active Directory 用户和计算机 MMC 管理单元	Dsa.msc	第 9 章，“设计 Active Directory 结构”第 11 章，“规划分布式安全”第 20 章，“将 Active Directory 与 Exchange Server 目录服务同步”第 24 章，“应用更改与配置管理”	此 MMC 管理单元是一个图形目录管理工具，它能让您可以在本单位目录中添加、修改、删除和组织 Windows 2000 用户帐户、计算机帐户、安全和分布组及发行资源。此工具安装在配置成域控制器的计算机上。
ApiMon	Apimon.exe	第 21 章，“测试应用程序与 Windows 2000 的兼容性”	一个为应用程序编程接口 (API) 调用计数、计时的应用程序监视工具。使用监视器报告 API 调用计数和每个调用的计时或按发生顺序跟踪报告 API 调用。可以在 Microsoft® Windows® 2000 Resource Kit 工具帮助中找到此工具。
* ClonePrincipal	Clonepr.dll Clone-gg.vbs	第 9 章 “设计 Active Directory 结	用于域迁移的工具。使用此工具把用户或组从 Microsoft® Windows NT® 4.0

	Clone-ggu.vbs Clone-lg.vbs Clone-pr.vbs Sidhist.vbs ADsSecurity.dll ADsError.dll	构”第 10 章 “确定域迁移策略”	版源域或 Windows 2000 源域复制到 Windows 2000 本机模式域，无需删除源帐户。原始帐户安全标识符 (SID) 添加到新帐户历史中，以便维持资源访问。
* Clustcfg	Clustcfg.exe	第 18 章，“确保应用程序和服务的可用性”	Windows 群集必需的配置工具。
*连接管理器	工具包	第 7 章，“确定网络连接策略”	一个基于图形的工具，它能让您创建自定义连接软件包，简化客户配置。
* Dependency Walker	Depends.exe	第 21 章，“测试应用程序与 Windows 2000 的兼容性”	扫描应用程序需要的所有非独立模块的工具。此工具检测诸如文件丢失或文件无效之类的问题。Dependency Walker 用于调试为 Windows 2000 编写或转换的应用程序。
*磁盘管理器	Windisk.exe	第 15 章，“升级和安装成员服务器”	Microsoft® Windows NT® 系统上提供的基于图形的磁盘管理工具。此工具允许您备份和还原磁盘配置信息。
*磁盘碎片整理程序 MMC 管理单元	Compmgmt.mmc	第 19 章，“确定 Windows 2000 存储管理策略”	此 MMC 管理单元允许您定位已经变为碎片的文件和文件夹，并在磁盘卷上重新组织簇。可以组织簇，这样文件、目录和可用空间在物理上更连续。
*磁盘管理 MMC 管理单元	Compmgmt.mmc	第 19 章“确定 Windows 2000 存储管理策略”	此 MMC 管理单元是管理磁盘和卷的图形工具。它支持分区、逻辑驱动器、新建动态卷和远程磁盘管理。
*组策略 MMC 管理单元	Gpedit.msc	第 11 章 “规划分布式安全” 第 12 章 “规划公钥基础结构” 第 23 章 “定义客户管理与配置标准” 第 24 章 “应用更改与配置管理”	此 MMC 管理单元是一个图形组策略管理工具，它能让系统管理员能够为特定用户组创建特定桌面配置。组策略设置定义用户桌面的不同组件，例如，用户可用的程序、出现在用户桌面上的程序和“开始”菜单选项。
Internet Explorer 管理工具包 (IEAK)	工具包	第 23 章，“定义客户管理与配置标准”	让您可以自定义 Microsoft® Internet Explorer 配置和设置的一套工具。备注 IEAK 不包含在 Windows 2000 中。有关 IEAK 的详细信息，参见本章后面的“其它资源”。
* Ipconfig	Ipconfig.exe	第 6 章，“为	基于字符的 TCP/IP 配置和诊断工具。

		Windows 2000 准备网络基础结构” 第 15 章，“升级和安装成员服务器”	使用此工具验证新升级的 Windows 2000 系统上的 TCP/IP 配置参数。例如，可以验证 IP 地址、子网掩码和默认网关。
*Internet 信息服务 MMC 管理单元	iis.msc	第 15 章，“升级和安装成员服务器”	Microsoft® Internet 信息服务 (IIS) MMC 管理单元是一个强大的站点管理工具，它能提供所有服务器设置的访问。使用 IIS 管理单元管理您企业 Intranet 上的复杂站点，在 Internet 上发布信息。
* LDAP 数据交换格式	Ldifde.exe	第 9 章，“设计 **Active Directory** 结构”	进行 Active Directory 数据大批输入和输出的命令行工具。
* Microsoft 许可证服务器	Licmgr.exe	第 16 章，“部署终端服务”	存储、跟踪并使 Windows 2000 终端服务客户访问许可证生效的工具。
Microsoft 管理控制台 (MMC)	Mmc.exe	第 1 章，“Windows 2000 部署规划简介” 第 9 章，“设计 Active Directory 结构” 第 10 章，“确定域迁移策略” 第 11 章，“规划分布式安全” 第 12 章，“规划公钥基础结构” 第 15 章，“升级和安装成员服务器” 第 16 章，“部署终端服务” 第 19 章，“确定 Windows 2000 存储管理策略” 第 20 章，“将 Active Directory 与 Exchange Server 目录服务同步” 第 23 章，“定义客户管理与配置标准” 第 24 章“应用更改与配置管理”	一个作为管理工具宿主的图形框架。可以使用 MMC 管理单元管理网络、计算机、用户、服务和其它系统组件。
* Microsoft 网络监视器	Netmon.exe	第 8 章，“使用 Systems Management Server 分析网络基础	收集并分析网络数据的图形工具。此工具允许您跟踪网络通信模式，在局域网

		结构 ”	(LAN) 上诊断网络问题。
Muisetup	Muisetup.exe	第 23 章，“ 定义客户管理与配置标准 ”	用于配置 Windows 2000 多语言版本的工具。可以更改默认用户界面 (UI) 或用 Muisetup.exe 添加或删除 UI 语言。
* Netdom	Netdom.exe	第 10 章，确定域迁移策略	允许您从命令行管理 Windows 2000 域和信任关系的域管理工具。也可以用此工具控制计算机域成员身份。
* Ping	Ping.exe	第 15 章，“ 升级和安装成员服务器 ”	基于字符的 TCP/IP 配置和诊断工具。此工具用于验证 TCP/IP 配置和诊断连接故障。
*远程安装服务(RIS)	工具包，包含 RISetup.exe RIPrep.exe RBFG.exe OSChooser.exe	第 24 章，“ 应用更改与配置管理 ”	该工具包允许您创建自定义 Windows 2000 Professional 映象，在远程安装服务 (RIS) 上设置这些映象并使用组策略在客户计算机上自动安装。
注册表备份	Regback.exe	第 15 章，“ 升级和安装成员服务器 ”	此工具在 Microsoft® Windows NT® Server Resource Kit 及Microsoft® Windows® 2000 Server Resource Kit 附带的 CD 上。此工具把注册表备份到文件，无需使用磁带。这样万一配置有问题，您也可以还原原始注册表设置。如同对任何重要数据一样，您需要经常备份注册表，特别是在安装和测试稳定性未知的应用程序之前。 可以使用 Regrest.exe 还原注册表，Regrest.exe 也可以在前面段落提到的 CD 上找到。
*路由和远程访问 MMC 管理单元	Rrasmgmt.mmc	第 7 章，“ 确定网络连接策略 ”	此 MMC 管理单元是管理和配置 Windows 2000 路由和远程访问的图形工具。
*安装管理器	Setupmgr.exe	第 13 章，“ 服务器自动安装与升级 ” 第 18 章，“ 确保应用程序和服务的可用性 ” 第 25 章，“ 客户机自动安装与升级 ”	帮您创建无人参与脚本的向导工具。安装管理器也创建无人参与和 Sysprep 部署需要的网络分布共享。

* Setupcl	Setupcl.exe	第 13 章，“ 服务器自动安装与升级 ”	此命令行工具与 Sysprep 一起工作，准备主控计算机上的硬盘，这样磁盘映

		第 25 章，“客户机自动安装与升级”	像工具可以把硬盘映像到其它计算机上。此工具重新生成新的安全标识符 (SID)。
SMS 安装服务	工具包	第 14 章，“使用 Systems Management Server 部署 Windows 2000”	一个为软件分发准备应用程序的 Microsoft® Systems Management Server (SMS) 工具。SMS 安装服务可以生成能够完全自定义的有人参与安装和无人参与安装脚本。
SMS Query Extract	用于 Microsoft Access 的 SMSExtract.mdb 用于 Microsoft Excel 的 SMSextract.xls	第八章，“使用 Systems Management Server 分析网络基础结构”	允许您在 Microsoft® Access 或 Microsoft® Excel. 中使用 SMS 查询的 SMS 数据抽取工具。
* Sysprep	Sysprep.exe	第 2 章，“创建部署路线图” 第 13 章，“服务器自动安装与升级” 第 18 章，“确保应用程序和服务的可用性” 第 23 章，“定义客户管理与配置标准” 第 24 章，“应用更改与配置管理” 第 25 章，“客户机自动安装与升级”	启动磁盘复制的安装工具。Sysprep 允许您安装有 Windows 2000 应用程序的系统，然后把它复制到其它系统。

*终端服务客户创建器	Tsclient.exe	第 16 章，“部署终端服务”	在以下操作系统上为终端服务客户软件创建软盘的图形工具：用于工作组的 Microsoft® Windows®，Microsoft® Windows® 95，Microsoft® Windows® 98 和 Microsoft® Windows NT® Server。
*终端服务配置 MMC 管理单元	Tscc.msc	第 16 章，“部署终端服务”	此 MMC 管理单元允许您管理终端服务配置。使用此工具修改的选项是全局性的，除非您选择从位于用户配置中的相同选项中继承信息。
*终端服务管理器	Tsadmin.exe	第 16 章，“部署终端服务”	允许您管理所有运行终端服务的 Windows 2000 Server 的图形工具。使用此工具，管理员可以查看当前用户、服务器和处理器。另外，还可以将消息发送到特定用户、使用远程控制功能和

			终端进程。
*工具管理器	Utilman.exe	附录 E，“供残疾人使用的辅助功能”	此工具让管理员能够指定 Windows 2000 启动时哪些计算机自动打开辅助功能工具。
Windows DNA 性能工具包	工具包	第 18 章，“确保应用程序和服务的可用性”	这套工具让您能够测试并调整应用程序的性能。该工具包包含组件服务和 IIS 的性能信息以及模拟许多用户同时访问组件服务或 IIS 应用程序的影响的工具。有关这套工具的详细信息，参见本章后面的“其它资源”。
* Windows 安装服务	内置服务	第 1 章，“Windows 2000 部署规划简介” 第 24 章“应用更改与配置管理” 第 25 章，“客户机自动安装与升级” 附录 A，“规划表示例”	使多个计算机上应用程序安装标准化的强大的 Windows 2000 安装服务。Windows 安装服务使用有 .msi 扩展名的软件包文件安装应用程序。
*Windows 管理规范	内置接口	第 1 章，“Windows 2000 部署规划简介” 附录 A，“规划表示例”	Windows 2000 管理基础结构，通过一般接口支持监视和控制系统资源并提供逻辑上组织好的、一致的 Windows 操作、配置和状态模型。使用 Windows 管理规范 (WMI),管理员可关联本地或整个单位的多个来源的数据和事件。WMI 允许您访问 Windows 2000 对象来创建自定义应用程序和管理单元。
*Windows Script Host (WSH)	Cscript.exe Wscipt.exe	第 1 章，“Windows 2000 部署规划简介” 附录 A，“规划表示例”	一个支持从用户界面或命令行直接执行 Microsoft® Visual Basic® Script、Java 和其他脚本的工具。
WinInstall LE	工具包	第 24 章，“应用更改与配置管理”	一个来自 Veritas Software 用于 Windows 安装服务的图形重新打包工具。此工具允许您迅速、方便地把现有应用程序（Windows 安装服务前的）重新打包到适合使用 Windows 安装服务分发的软件包。
* Winnt	Winnt.exe	第 13 章，“服务器自动安装与升级” 第 25 章，“客户机自动安装与升级” 附录 B，“安装命令” 附录 C，“无人参与安装的应答文件示	可用于在运行 Microsoft® MS-DOS® 或 Microsoft® Windows® 3.x 的计算机上新安装 Microsoft® Windows® 2000 Server 或 Microsoft® Windows® 2000 Professional 的安装命令。

		例 ”	
* Winnt32	Winnt32.exe	第 13 章，“ 服务器自动安装与升级 ” 第 25 章，“ 客户机自动安装与升级 ” 附录 B，“ 安装命令 ’ 附录 C，“ 无人参与安装的应答文件示例	可用于在运行 Windows NT 4.0, Windows 95, 或 Windows 98 的计算机上新安装或升级至 Windows 2000 Server 或 Windows 2000 Professional 的安装命令。

其它资源

- 有关 IEAK 的详细信息，参见 Web 资源页的 “Microsoft Internet Explorer Administration Kit (IEAK)” 链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources。
- 有关 Windows DNA 性能工具包的详细信息，请参见 Web 资源页的 “Windows DNA 性能工具包” 链接，网址是：http://windows.microsoft.com/windows2000/reskit/webresources。

附录 E - 供残疾人使用的辅助功能

Microsoft 致力于让所有人都能平等地访问并使用其产品和服务。Microsoft® Windows® 2000 新增及增强的辅助功能，让各行各业的用户都从中受益。这些功能，使用户能更容易自定义计算机，以让残疾用户能更好地使用程序和应用程序，完成自己的工作。

本附录内容

Windows 2000 辅助功能概述
部署 Windows 2000 辅助功能
自定义计算机辅助功能选项
配置 Windows 2000 辅助功能
根据残疾类型设置选项

附录目标

本附录将帮助您完成以下目标：

- 制定为残疾用户安装操作系统内置功能及第三方附件设备的规划。
- Windows 2000 升级需要考虑的优选组件及功能列表。

资源工具包中的相关信息

- 有关软件安装的更多信息，请参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide* 中的“Software Installation and Maintenance”。
- 有关“组策略”的更多信息，请参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide* 中的“Group Policy”。

Windows 2000 辅助功能概述

辅助功能旨在让每一个人，包括那些有认知、听力、身体或视觉障碍的人，都能平等地使用计算机软件。认知障碍包括：学习障碍、唐氏综合症、诵读困难及语言缺陷（如文盲）。听觉障碍包括：失聪及听力不好。身体障碍包括：脑中风、发抖、癫痫症发作、手指或脚趾残缺以及麻痹症。视觉障碍包括：失明、各种视力低下（如色盲、以及管状视症）。Windows 2000 的辅助功能，旨在通过灵活的、可自定义的用户界面、各种替代输入输出方式、以及屏幕元素更好的可见性，使计算机更容易操作。

Windows 2000 辅助功能的优点

随着使用计算机的残疾人士增加，愈发要求其雇主向他们提供辅助性技术。最近的立法，包括 1998 年的 Workforce Investment Law （《劳动力投资法案》），就有此要求。残疾员工必须能最大限度地象正常员工一样使用计算机。为此，Windows 2000 内置了多项技术，使企业可以为计算机配置需要的辅助功能。

其中，很多功能都是 Microsoft® Windows® 98 和 Microsoft® Windows NT® 操作系统所没有的。本附录阐述了已有的、及新增的功能。Windows 2000 中的一些新增的或显著增强的功能及工具包括：Microsoft® Active Accessibility®、“辅助功能向导”、“放大镜”、“讲述人”、“屏幕键盘”、“工具管理器”、高可见性鼠标指针、同步可访问媒体互换（SAMI）及高对比度颜色方案。

用 Windows 2000，用户及管理员能实现以下功能：

为用户自定义设置重设默认值。通过“控制面板”、“辅助功能向导”及“工具管理器”，管理员可为几组用户设置广泛的辅助功能。

进行快捷、方便的 Windows 导航。一些特殊功能（如热键、Active Desktop™ （活动桌面）等）使访问桌面对象、“资源管理器”、网络上的其它服务器以及 Internet Explorer 更加容易；有助于快速进入 Windows；有助于帮助打开文件夹及建立个性化的设置。

使用更为广泛的辅助技术。通过 Microsoft Active Accessibility，应用程序可以与第三方及其它附件辅助设备（如语音识别系统及其它形式的辅助设备）更有效地工作。Active Accessibility 已暗中升级和扩展了 Microsoft Windows 操作系统。

自定义输入法。键盘的扩展配置（包括“屏幕键盘”、特殊鼠标设置及其它选项）让用户能自定义用户界面方案。

通过单一入口点配置选项。位于“开始”菜单中的“辅助功能向导”，使管理员及用户可以在计算机上安装最常用的功能，并让每一位用户自定义这些功能。

放大显示屏幕的某一部分。几项简单的功能（如“放大镜”），让用户在工作时能丢开平时的辅助设备。

让 Windows 更加机动灵活。键盘快捷键及个性化的键盘选项，可以帮助用户使用程序及应用程序。

设置声音选项适合不同的听力要求。除了可自定义的功能之外（如音量调节、多媒体选项），还有一些辅助功能，如“声音显示”和“声音卫士”，让有听力障碍的人士可以控制他们的声音环境。

为有视觉要求的用户设置选项。这些功能包括：“讲述人”，它是一个操作系统内置的“文本到语音”工具；“切换键”，当用户按下某些锁定键时，会发出声音提示；以及“控制面板”的“声音与多媒体”图标处的事件提示功能。

通过键盘筛选键自定义键盘按键，为有不同认知、听觉、灵活性及视觉需要的用户提供帮助。“切换键”功能可调整键盘响应时间，忽略无意的按键。

设置屏幕元素的对比度、颜色、调速及尺寸方案。高可见性的鼠标指针、高对比度的颜色方案、以及“辅助功能向导”等扩展屏幕元素，给用户提供了一些选项，可以适合不同的需求及偏好。如让插入点指针（有时称为“脱字符”）有更好的可见性，或关掉动画。

通过使用第三方设备，对个人计算机更好地控制。“串行键”功能是专为那些不能使用标准 UI 选项、但需要增强设备协助的人士设计的。此功能允许用户把替代输入设备连到计算机的串行端口。

升级至 Windows 2000 之前的注意事项

Microsoft 和其它软件及硬件开发商一直不断努力，致力于改进针对残疾人士的选项。也正由于这种努力的长期性，在新版的软件发布时，有些辅助功能可能还在开发或测试中。有时，新的功能是在软件发布后才完成的，因此只能加到下一个版本中。此外，有些技术还不能与 Windows 2000 兼容，或不能内置于 Windows 2000 中。由于这些原因，信息技术的专业人士在对那些有辅助功能要求的企业进行部署之前，应该认真回顾支持哪些用户需求。作为部署规划和测试的一部分，请务必测试所有的辅助设备与 Windows 2000 的兼容性。

您可以以考虑对部分现有的功能及程序进行升级，而不是完全安装 Windows 2000。升级过程可以自动完成，并可以通过 Active Directory™ 目录服务来管理部门、域或站点中的组策略对象应用程序。尽管完全安装（有时也称为原始安装）允许分区组合，但它不会迁移原操作系统的设置，这意味着用户将失去其个性化的设置及应用程序。

备注 无论是进行完全安装，还是升级，都必须使用与 Windows 2000 兼容的已升级的基本输入/输出系统 (BIOS)，这一点很重要。

通过在“ 组策略 ”中指定应用程序，管理员可以公布对象，这样当用户从“ 开始 ”菜单上选中这些对象时，它们将会自动安装。管理员也可以删除用这种方法指定的应用程序。如果管理员是“ 发布 ”而不是“ 指定 ”了这些应用程序，用户可以选择通过“ 控制面板 ”中的“ 添加/删除程序 ”进行安装。建立在组件对象模型 (COM) 基础上的 Active Accessibility 是 Windows 操作系统的核心组件，由它来定义应用程序进行用户界面元素信息交换的方式。这项技术降低了某些辅助功能的不兼容的可能性，但它还不能提供完全的兼容性。有关当前技术的更多信息，请参见 Web 资源页的“ Microsoft Accessibility ”链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

有关软件安装的更多信息，请参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide* 中的“ Software Installation and Maintenance ”。

部署 Windows 2000 辅助功能

虽然 Windows 2000 发布的一些辅助功能工具，为那些有特殊需求的用户提供了一些功能，但大部分残疾用户日常工作仍需要功能更强的辅助功能。通过使用独立供应商开发的硬件及软件，残疾人士可以加强对 Windows 操作系统的使用。请务必测试 Windows 操作系统与辅助功能程序、应用程序及设备的兼容性，以确定其驱动程序与 Windows 2000 兼容。

Microsoft Active Accessibility

Active Accessibility 应用程序编程接口内置于 Windows 操作系统中。 它基于 OLE 及 COM，在用户使用界面元素时提供了辅助配合。对用户来说，Active Accessibility 是不可见的。该项技术有助于某些辅助功能的兼容性。

第三方产品和服务

Microsoft 与独立的厂商合作，为残疾用户生产了兼容软件及硬件。Active Accessibility 功能的目标之一就是，提供一个基础结构，帮助操作系统和应用程序互相理解，以使这些重要的设备具备更好的兼容性。通过“ 工具管理器 ”（ Windows 2000 的一个新功能），供应商现在能够将他们的产品添加到计算机，让它们更好用。

独立供应商，一般是那些专门制造辅助设备的小公司，帮助残疾人士更好地使用 Windows 操作系统。下面列出了一部分由独立供应商生产的设备和功能类型。

- 修改鼠标和键盘行为的硬件和软件
- 屏幕键盘
- 允许用户通过鼠标或语音激活方式输入的程序
- 通过预测单词或短语，让用户以更少的击键更快地输入的软件
- 有显示字幕的程序
- 替代输入设备，如头点器、 单一按键、目控定点设备、吸吹器及语音输入设备。
- 放大或改变屏幕信息颜色的程序

- 合成语音程序，或把信息显示在屏幕上的 Braille 浮点打印机

“Windows 认证”徽标

业内的硬件及软件供应商正共同努力，旨在为所有计算机用户提供更好用的产品。Microsoft 最早提出了“Windows 认证”程序，现用于 Windows 2000。该程序促进了更易用的设计方案的出现，同时它包括了对应用程序开发商的一组要求及校验表。该程序的主要目标是，保证用于 Windows 2000 操作系统的产品的质量及一致性。要达到“Windows 认证”徽标的要求，应用程序必须通过 VeriTest 的“ Windows 2000 应用程序规范”测试。

规范阐述了如下的要求，如替代只能依赖语音传递信息的显示字幕；插入点指针（也称为“脱字符”）的可见性；通过控制鼠标及键盘来关闭动画的能力。这种合作努力的目标之一是确保残疾用户辅助设备的质量及一致性。

有关“Windows 认证”程序，包括应用程序规范的更多信息，请参见 Web 资源页的“Application Specification Download”链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

重要提示 大多数第三方辅助功只与特定版本的操作系统兼容。一些附件工具需要依赖某种文件格式及编程接口才能准确地向用户解释数据，这很惹人讨厌。这种依赖性根据操作系统的不同而有所不同。因此，在决定升级前， 获取清单信息并进行新操作系统和应用程序的兼容性测试是很重要的。有关日见增多的技术以及兼容性的更多信息，请参见 Web 资源页的“Microsoft Accessibility”链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

使用“串行键”外挂硬件和软件

“串行键”功能允许您将第三方辅助设备连接到计算机的串行端口。例如， 您可以把替代键盘或增强通信工具连接到个人电脑的串行端口。“串行键”功能是专为那些不能使用标准 UI 方法的人士设计的。但“串行键”也允许增强型设备与本地键盘和鼠标一起使用。

自定义计算机辅助功能选项

Windows 2000 会自动安装辅助功能选项。而且一旦安装，用户将无法从操作系统中将其删除，其中包括“控制面板”或“辅助功能向导”中的那些功能。除了新增功能外，当您从早期版本的 Windows 进行升级时，安装程序将默认保留已安装的功能。您也可以在共享计算机，如公用或工作组服务器上安装辅助功能。

从 CD 进行远程安装和无人参与安装

如果客户计算机支持远程安装，您可以使用“客户安装向导”远程安装计算机。通过“组策略”，可以对提供给用户的选项进行控制。这里有四种安装选项：自动安装，自定义安装，重新开始以前的安装尝试，维护与故障排除。

自动安装 在默认的“自动安装”选项中，Windows 2000 远程安装服务将使用无人参与安装模板，这样，您可以在操作系统映象目录中建立选项。使用无人参与安装的安装应答文件，还可以建立几个安装选项，选择要安装的项目，并配置特定客户计算机的选项。

自定义安装 使用“自定义安装”选项，您可以指定计算机名称，以及指定建立计算机帐户对象的 Active Directory 容器。该选项还可以为用户组中的个别用户安装计算机，也可在用户拿到计算机前，在 Active Directory 中设置一个客户计算机帐户。

重新开始以前的安装尝试 该选项将重新启动以前的或失败的安装尝试。例如，如果操作系统映射安装开始

后，与远程安装服务服务器的连接中断，您可以通过以下步骤继续该安装过程。重新启动客户计算机，在出现启动网络服务的提示时，按 F12 键，单击“ 重新开始以前的安装尝试 ”。

维护与故障排除 “ 维护与故障排除 ”功能让管理员能使用必要的诊断工具及其它的维护工具，对客户计算机进行维护及故障排除。

Windows 安装服务

作为一项在客户计算机上安装、维护及删除软件的技术，“ Windows 安装服务 ”为我们展示了自我修复型的应用程序。如果用户试图删除一个文件，但后来又想打开它，“ Windows 安装服务 ”将恢复丢失的文件。有关“ Windows 安装服务 ”的更多信息，请参见 Web 资源页的“ Windows Platform Software Development Kit (SDK) ”链接，地址是： http://windows.microsoft.com/windows2000/reskit/webresources。

组策略

“ 组策略 ”是网络管理员管理用户组及计算机组的主要工具。管理员可通过 Microsoft® 管理控制台 (MMC) 的“ 组策略 ”管理单元，来指定被管理的计算机组及用户组的桌面管理及安全选项。Microsoft® Windows® 2000 Server 包括了 200 多个组策略的默认设置。使用“ 客户安装向导 ”，可以指定用户安装选项，并允许或禁止用户对某些指定的选项访问。“ 组策略 ”对一个有残疾用户的企业是很重要的，因为可以使用它，为那些有相同辅助需求的用户组一起定义设置。同时，同一台计算机的多个用户可以通过不同的登录及密码信息，设置自己的的桌面喜好，包括某些辅助功能选项。

有关使用“ 组策略 ”的更多信息，请参见 *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide* 中的“ Group Policy ”。

设置多用户配置文件

您可以通过“ 辅助功能向导 ”设置多用户配置文件。当下一用户登录到 Windows 时，不需要删除以前的设置，就可修改设置。当以前用户再一次登录时，个人设置将还原。这项功能使用户或管理员能设置用户喜好的参数。Windows 为其他用户自动将功能预设为默认值。当辅助功能关闭后，不需要这些功能的用户不会注意到已安装了这些功能；因此，需要以及不需要这些功能的用户匀能使用这台计算机。同一台计算机的多个用户，可通过各自的登录及密码信息来设置他们的喜好及桌面设置，包括任何需要的辅助功能。

管理选项

使用“ 控制面板 ”或“ 辅助功能向导 ”，您可以对多项功能设置管理选项。 这里有两项您匀可设置：设置自动超时/自动复位、默认辅助功能设置。但如果您想把设置存在一个文件中，以便在另一台计算机上也能使用，就必须使用“ 辅助功能向导 ”。

辅助功能复位（超时）

多个用户共享的计算机另一个有用的功能是“ 辅助功能复位 ”超时功能。在“ 辅助功能向导 ”及“ 控制面板 ”中都有该组件；如果计算机空闲超过一定时间，其辅助功能将被关闭。然后，操作系统将回到默认配置。

备注 “ 自动复位 ”（超时）功能不会关闭“ 串行键 ”功能。

活动桌面

通过“ 活动桌面 ”，除了显示 intranet 及 Internet 内容外，用户还可以对桌面上几乎所有的东西个性化处理。Windows 2000 “ 资源管理器 ”让用户能在桌面元素间转来转去，比如任务栏图标、文件和快捷方式

图标，及网络上的其它对象。这项功能，为所有类别对象提供了一致的界面，同时对某些用户来说，这比使用鼠标在桌面对象间跳转更容易。

自定义桌面

下面的几个例子中，用户可以通过以下方式用 Active Desktop 自定义桌面。

- 把含有活动内容的 Web 页添加到桌面。
- 把工具栏放在桌面或任务栏上一个更便捷的地方。
- 重新组织经常打开的文件及程序，以便快速访问。
- 在任务栏或桌面上添加地址。通过添加地址，用户就不用先打开浏览器，再键入一个 Internet 地址。

桌面工具栏

用户可以用他们常用的命令创建桌面工具栏。这对更喜欢用鼠标而不是键盘的用户来说，是最有用的；喜欢键盘的用户一般都想把命令添加到“开始”菜单。

系统状态图标

能在任务栏（有时被称作“系统托盘”）系统状态区的状态图标间切换，是 Windows 2000 新添的功能。 当用户激活常用辅助功能的状态图标时，它们将会出现在系统状态区。此外，当用户按下键盘快捷键时，图标将出现在相应的矩形内，显示出被激活的键。这些状态图标取代了 Windows 早期版本中的状态指示器。

工具管理器

Windows 2000 新添的“工具管理器”使用户能节省时间。管理员能指定哪些计算机在 Windows 2000 启动时，自动打开辅助功能工具。然后，用户可以停止或重新启动这些工具，以适合他们的需要。对某些用户来说，能即时使用像“讲述人”、“放大镜”或“屏幕键盘”等功能是很重要的。

用户和管理员也可以通过“工具管理器”，对计算机上的大部分辅助功能程序进行自定义。管理员可打开一个对话框，查看都安装了哪些 Windows 2000 辅助功能工具，及其现在的状态。管理员也能安装其它的应用程序，或运行安装附件设备的程序。尽管可以通过“开始”菜单进入“工具管理器”，但可以用一种更快的方式打开它，即使用下列快捷键：“WINDOWS 徽标” + U.

备注 可以从“工具管理器”打开的内置程序包括：“放大镜”、“讲述人”和“屏幕键盘”。除了 Microsoft 内置在操作系统中的应用程序外，第三方供应商也可把应用程序添加到“工具管理器”。

有关向“工具管理器”添加增强设备的更多信息，请参见特定第三方工具的相应文档。

在 Windows 2000 中配置辅助功能

通过建立自定义的界面，残疾用户能控制他们的计算机环境，以便使用需要的软件完成各自的工作。视各人需求的不同，用户可能会觉得 Windows 在不同的方面有挑战性。虽然辅助功能在完全安装 Windows 2000 时是自动安装的，但是原来的配置选项和设置都必须重新配置，而且要为不同用户配置好新的自定义选项。

表 E.1 描述了 Windows 2000 操作系统中内建的一些辅助功能。鉴于有些功能可用于几种残疾，因此这些功能是根据特定的困难而不是根据残疾类型列出的。有关根据残疾类型分类的功能描述，请参见本章稍后的“根据残疾类型设置选项”。

表 E.1 一般的用户困难及解决方案

用户困难：	Windows 2000 解决方案
在多用户网络中自定义设置。	“辅助功能向导”、“管理选项”、“控制面板’中”辅助功能选项”。
执行以下任务： • 打开 Windows 或应用程序。 • 在桌面元素及 Windows 中跳转。 • 自定义键盘设置。 • 自定义显示设置。	热键、“工具管理器”、“讲述人”、“屏幕键盘”、“活动桌面”、键盘快捷键、系统状态图标。
记住已激活的辅助功能。	“控制面板”中的”辅助功能选项”。
查找所需功能。	“辅助功能向导”，根据残疾类型列出各功能。
记住键盘导航指示器。	“辅助功能向导”、“控制面板”中的“辅助功能选项”及“显示”。
正确拼写单词。	“自动拼写检查程序”、“自动填写”功能、“自动更正”功能、键盘快捷键。
听力，比如以下情形： • 听声音提示。 • 区分声音。 • 听发声提示。 • 在嘈杂的环境中工作。	“声音显示”、“声音卫士”、自定义声音方案
使用标准键盘配置。	Dvorak 键盘、“屏幕键盘”、“鼠标键”
因为反应慢而使用了键盘。	“重复键”和键盘选项
无意的击键或回弹键。	“慢键”、“回弹键”、“重复键”及“切换键’
同时按下两个键。	“粘滞键”
使用标准用户界面方法，包括鼠标和键盘。	第三方语音输入工具、“讲述人”、“屏幕键盘”
操纵鼠标。	“鼠标键”
遇到闪烁事件和其它方案会引起疾病发作。	“控制面板”中的”辅助功能选项”，允许用户改变调速、声音方案、颜色及对比度；以及“辅助功能向导”。

看见或跟踪鼠标指针。	“ 控制面板 ”或“ 辅助功能向导 ”中的“ 鼠标 ”选项
看见键盘状态光亮。	“ 切换键 ”
看见屏幕元素。	“ 讲述人 ”、“ 放大镜 ”、“ 控制面板 ”、及“ 辅助功能向导 ”中的尺寸、颜色、对比度方案。
正常使用内置的辅助功能（需要附件设备）。	Active Accessibility、针对第三方辅助设备的“ 串行键 ”
查找第三方辅助设备及其它辅助功能信息。	Microsoft Accessibility Web 站点（详细内容，请参见本附录中的“ 额外资源 ”）。

通过“ 控制面板 ”中的 ”辅助功能选项 ”，用户及管理员可自定义 Windows 2000 的许多辅助功能。但您现在可以通过“ 辅助功能向导 ”，对常用的辅助功能进行配置。例如，您既可以使用“ 控制面板 ”，也可以使用“ 辅助功能向导 ”，来自定义显示、键盘、鼠标及声音操作，以满足用户的特殊需要。在下面的小节中描述了配置选项的两种方法：

通过“ 辅助功能向导 ”配置辅助功能选项

“ 辅助功能向导 ”是 Windows 2000 新增的功能。通过它可以更容易地根据用户特殊的需要安装辅助功能选项，而不用通过改变数值或通过“ 控制面板 ”。该向导可以从“ 开始 ”菜单找到，它为许多常用功能提供了单一入口点。用户也可以把设置存放在一个文件中，用于配置其它的计算机。该向导控制的一些选项包括：声音和屏幕选项，如音量、字体大小；键盘选项，如键盘筛选键及“ 鼠标键 ”；以及设置管理选项的能力。

使用“ 控制面板 ”配置辅助功能选项

“ 控制面板 ”中的“ 辅助功能选项 ”图标，使用户能更容易地自定义一些属性，对 Windows 2000 中的许多辅助功能施加控制。用户可打开或关闭这些功能，并能自定义键盘、声音及鼠标选项以适应用户特定的需要。“ 辅助功能选项 ”让用户能使用下列功能：“ 粘滞键 ”、“ 筛选键 ”、“ 切换键 ”、“ 声音卫士 ”、“ 声音显示 ”、“ 鼠标键 ”及“ 串行键 ”。

除了 ”辅助功能选项 ”中为残疾用户提供的选项之外，“ 控制面板 ”还提供了修改客户计算机设置的其它的方法。用户可修改“ 显示 ”、“ 键盘 ”、“ 鼠标 ”、“ 声音与多媒体 ”等设置。下面几节描述了很多其它功能，以及专为残疾用户设计的功能。

根据残疾类型设置选项

通过建立自定义界面，残疾用户可以对他们的计算环境施加控制，以胜任工作。一个简化的用户界面对于减轻导航负担是很有必要的。以下是 Windows 2000 中的一些功能及技术，用户及管理员可以进行自定义，以适合特殊的需要及喜好。虽然很多选项适用于多种残疾，但出于布局的需要，把它们按残疾类型分类。

针对认知障碍用户的选项

认知障碍包括：发展障碍，如唐氏综合症；学习障碍，如诵读困难、语言不熟、文盲；注意力不足及记忆丧失；知觉困难，如反应慢。除了第三方辅助设备（如声音输入工具）外，Windows 内置的一些功能对有认知障碍的人会非常有帮助。其中比如一些 IntelliSense® 功能，包括“ 自动更正 ”、“ 自动填写 ”及“ 自动

拼写检查 ” 等。

您可自定义 “ 自动填写 ” 功能，让它只加入用户需要的信息。对有些用户来说，这些功能将极大地促进他们的工作。但对其他的用户来说，（如有认知障碍的用户），如果能清除而不是选用这些功能（如 “ 自动填写 ” 及有些声音方案）将更为有利。这些功能会使人分心，尤其是对使用 “ 文本到语音 ” 工具的用户。

对有认知障碍的用户来说，“ 控制面板 ” 或 “ 辅助功能向导 ” 中的一些 Windows 2000 辅助功能是很有用的。熟悉 Windows NT 4.0 及更早版本的用户应该了解，Windows 2000 的键盘筛选键已做了调整。“ 辅助功能向导 ” 及 “ 控制面板 ” 都允许用户调整键盘的响应时间，使其忽略无意的按键及慢的响应时间。

对有认知障碍的人有用的键盘选项包括：热键，及其它键盘快捷键。此外，以下功能对有认知障碍的人也是有用的：“ 讲述人 ”；“ 活动桌面 ”；能显示哪些功能已被激活的系统状态图标；“ 控制面板 ” 和 “ 辅助功能向导 ” 中的 “ 声音 ” 选项。而且，声音方案有助于吸引注意力，或向用户提供有关任务的额外反馈。

同步可访问媒体互换

有语言方面困难的用户可能会发现， Microsoft 的 “ 同步可访问媒体互换 ” （SAMI）是很有用的，它能让您通过文本字幕，更好地理解声音。Windows 2000 的这个功能将在本附录后面的 “ 针对听力障碍用户的选项 ” 一节中加以阐述。

针对听力障碍用户的选项

对于耳聋或听力差、声音分辨力不足的用户，下列选项很有用。这些功能包括，声音方案调整或替代声音的可视媒体。

可自定义的声音方案

听力不好的用户，或在嘈杂环境工作的用户，可以调整音高及音质，调整屏幕事件关联音量，使它们更容易辨别。这些声音可以通过 “ 辅助功能向导 ” 或 “ 控制面板 ” 进行自定义。

Windows 向用户提供了能与许多事件相关联的声音。这些事件可能是由 Windows 或程序产生的。如果用户对区分默认声音（如无效击键的提示音）有困难，他们可选择新的声音方案，或设计自己的声音方案，以便能更容易地辨别声音。Windows 2000 允许用户能关闭下载默认的声音文件。

调节音量

如果计算机装有声卡，用户可通过 “ 控制面板 ” 中 “ 声音与多媒体 ” 图标，调节所有的计算机声音音量。也可通过任务栏的扬声器图标，或 “ 音量控制 ” 来调节音量。

有些用户要求有视觉反馈替代声音。失聪的用户把手语作为主要语言，而把英语当作第二语言。他们在阅读使用自定义字体的页面、不合印刷常规的页面（如大小写混写）或显示动画文字的页面时，可能会遇到困难。在这种情况下，用户能从可自定义的声音及显示字幕中受益。

以下 Windows 2000 功能对失聪或听力不好的用户很有用。

声音显示

“ 控制面板 ” 中的 “ 声音显示 ” 功能，让应用程序以显示字幕的方式来显示视觉反馈。在 Windows 2000 中，用户可选择显示字幕。

声音卫士

Windows 2000 中，“ 声音卫士 ”功能只支持由计算机内部扬声器产生的声音；它无法检测由多媒体声卡发出的声音。如果计算机装有多媒体声卡，用户或管理员可能需要将它关闭，让计算机内置的扬声器发声。这样，“ 声音卫士 ”就能检测到这些声音事件。要使该变化生效，用户需要重新启动 Windows。

同步可访问媒体互换

Microsoft “ 同步可访问媒体互换 (SAMI) /直接显示 ”用于显示字幕。SAMI 是开发者、教育工作者、及 Web 作者可在单一文档中用来编制字幕及声音描述的一种格式。SAMI 基于 HTML 来提供熟悉的可阅读的格式。用 SAMI，开发者及其他人就能建立有显示字幕的多媒体产品。桌面上的“ Windows 媒体播放器 ”向用户同步提供字幕信息，然后用户可以调整字幕，以适合个人需要。

有关 SAMI 的更多信息，请参见 Web 资源页的“ Microsoft Accessibility ”链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

针对身体残疾用户的选项

有些用户可能无法完成一些手动任务，如使用鼠标，同时敲击两个键等。有些用户则可能会敲击好几个键，或手指回弹。身体残疾或灵活性损伤包括：瘫痪、反复性的紧张、脑中风、动作不听使唤，四肢麻痹及手指或脚趾残缺。很多用户需要调整键盘及鼠标功能，以适合他们特殊的需要，或者可能需要依赖某种专门替代输入产品。幸运的是，有很多替代输入设备可供用户选择，包括通过用户的声音控制计算机的语音输入工具、键盘筛选键、屏幕键盘，更小或更大的键盘、眼控指针设备，以及可以通过呼吸控制的“ 吸吹 ”系统。有关辅助设备和第三方辅助设备编录的更多信息，请参见 Web 资源页的“ Microsoft Accessibility ”链接，地址是： http://windows.microsoft.com/windows2000/reskit/webresources。

键盘选项

灵活性损伤可能使一个人在用标准键盘时遇到困难；Windows 2000 内置的键盘筛选键通过纠正颤抖动作和慢的响应时间在一定程度上弥补了类似情况造成的困难。其它的键盘筛选键包括辅助输入，如单词预测、缩写词扩展工具及附加拼写检查工具。以下各节阐述了与标准键盘不同的输入设备及功能。这些功能包括一些选项，能调整按键的方式，以满足对特殊的辅助功能的需要。

备注 在大多数情况下，不可能把同样的键盘行为纠正应用到指针设备如鼠标上。这一限制了又让有灵活性障碍的用户只能使用键盘输入。

屏幕键盘

有些用户对使用鼠标及键盘都有困难。但他们能通过另外一种输入方法来使用屏幕键盘，比如指针设备、与串行端口连接的操纵杆、或将键盘空格键作为一个切换设备。屏幕键盘这个工具，允许用户通过使用一个替代输入方式来选择按键。能指向却不能点击的用户，可以使用指针工具、切换器或“ 摩斯码 ”输入系统。

备注 您需要把接插线自定义为切换模式。

通过“ 开始 ”菜单，用户可以安装并自定义 Windows 2000 “ 屏幕键盘 ”。对有一般灵活性损伤的用户，“ 屏幕键盘 ”提供了最低限度的功能。但很多身体残疾的用户，日常工作需要功能更高的工具程序。有关基于 Windows 的屏幕键盘的更多信息，请参见 Web 资源页的“ Microsoft Accessibility ”链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

备注 “ 屏幕键盘 ”只是作为一个临时性的解决方案，并非作为日常的替代键盘可以替代第三方屏幕键盘。

Dvorak 键盘

对使用标准传统键盘布局有困难的人来说，使用 Dvorak 键盘的键盘布局，能更容易地敲击到常用的字符。有三种 Dvorak 布局：一种针对两只手敲击，一种针对只用左手敲击，一种针对只用右手敲击。 Dvorak 布局减少了输入一般英语文字所需的移动范围。这可能有助于克服与打字有关的重复性拉伤。您可将其作为安装程序的一部分添加 Dvorak 键盘，也可以以后再添加。要配置 Dvorak 键盘，请使用“ 控制面板 ”中的“ 键盘 ”图标。

键盘快捷键

键盘快捷键对残疾用户来说，是最重要的。对所有类型的残疾，它们都具有不可比拟的价值。这些 ALT 命令及 CTRL 键能帮助用户更容易地在 Windows 2000 中航行。即使没有配置辅助功能，用户还可以在对话框中使用 TAB 键，移动焦点，然后用箭头键在列表中选择项目。在有多个选项卡的属性页中，用户可从左到右选择每一个属性页。在“ 活动桌面 ”中，用户可以把快捷键添加到“ 开始 ”菜单中。

有关键盘快捷键（包括快捷键）的更多信息，请参见“ Windows 2000 帮助 ”。

有关键盘快捷键的更多信息（包括辅助键盘快捷键的详细列表），请参见 *Microsoft Windows 98 Resource Kit* 中的“ Appendix H – Accessibility ”。

有关只对键盘有效的命令、辅助快捷键以及 Microsoft® Natural® Keyboard （ Microsoft 人工键盘）的更多信息，请参见 Web 资源页的“ Microsoft Accessibility ”链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

辅助功能的热键

辅助功能的热键，为那些不先启用辅助功能便无法使用计算机的用户，提供了即时激活辅助功能的方法。作为一种快捷键，热键使用户能临时打开某一特定的功能。在打开了一个功能之后，用户可通过“ 辅助功能向导 ”或“ 控制面板 ”中的 ” 辅助功能选项 ”来调节该功能以适合个人的喜好，也可永久地打开该功能。如果别人使用这台计算机时不想用这个功能，或它妨碍了别人使用这台计算机，该热键也可临时关闭该功能。

热键设计成一些特殊键的组合，但不能与程序所用的键冲突。如果出现了冲突，用户可以关闭这些键，但还可使用所需的功能。在 Windows 2000 典型安装中，辅助功能热键处于非活动状态，以防止与其它程序发生冲突。

针对单指输入或嘴杖输入的粘滞键

很多软件程序要求用户同时按下两至三个键。 但对于只用一个手指或使用嘴杖的人来说，这是不可能的。“ 粘滞键 ”允许用户一次按下一个键，同时指令 Windows 象同时按下几个键那样，作出响应。

对于共享的计算机，有一个可选功能，即使该粘滞键没有关闭，其他的用户也不会由此产生使用上的混乱。如果“ 同时按下两个键将关闭沾滞键 ”选项被激活，当有两个键被同时按下时，“ 沾滞键 ”将会检测出这一点，并自动关闭沾滞键功能。

有人不喜欢键盘声音，而有人觉得有用。通过取消选择“ 沾滞键 ”属性中的“ 当按下修改键时发出声音 ”选项，用户可以关闭反馈声音。

针对手动灵活性损伤用户的筛选键

Windows 2000 包括了键盘筛选键，可单独使用，也用组合使用；对那些由于反应慢、异常动作颤抖、无意触键或手指回弹而对键盘使用感到有困难的用户，他们的输入会变地容易些。用“ 沾滞键 ”功能，用户可以调整键盘响应时间，允许无意间按键及慢的响应时间。

针对会无意碰到锁定键的用户的切换键

当 NUM LOCK、CAPS LOCK 或 SCROLL LOCK 锁定键被激活时，“ 切换键 ”会指令 Windows 发出或高或低的响声。响声将提醒用户，其中的一个键已被激活。

鼠标选项

有灵活性损伤的用户可以在尺寸、颜色、及动画方案中作出选择。在“ 控制面板 ”中的“ 鼠标 ”图标中，用户可以调整鼠标属性，以增加指针的可见性。这项可自定义的功能，虽然不只针对残疾用户，但对有视觉障碍的用户来说，是非常有用的。

调整鼠标属性

通过“ 控制面板 ”中的“ 鼠标 ”图标，用户可使鼠标指针自动移向对话框的默认按钮，如“ 确认 ”或“ 应用 ”；也可调整按钮，使其右键变为主键。用户还可对其它的鼠标设置进行调整，如指针移动及加速的速度；左右键调整；光标大小、颜色、形状、双击速度及动画。通过选择“ 我是有视力障碍的人 ”及“ 使用键盘或鼠标对我来说非常困难 ”，用户可以对“ 辅助功能向导 ”中的几项辅助功能“ 鼠标 ”选项进行设置。

针对只用键盘输入的鼠标键

虽然 Windows 2000 的设计原则是，所有动作即使不用鼠标也能完成，但有些程序还是要求用鼠标，而且对有些任务，使用鼠标会更方便。“ 控制面板 ”中的“ 鼠标键 ”对需要精确定位指针的制图人员及其他人是很有用的。用户不一定有鼠标才能使用这个功能。通过“ 鼠标键 ”，用户可以控制用一个手指、嘴杖，或通过数字小键盘的头点器来控制鼠标指针。以这种方式，用户可用鼠标的两个键来点击、双击或移动对象。“ 鼠标键 ” 激活之后，如果打开了声音，它就会发出一种升调。

针对触觉过敏用户的选项

对象癫痫症等有触觉过敏的用户，可通过 Windows 中的“ 控制面板 ”或“ 辅助功能向导 ”，调整屏幕元素，如调速、颜色、对比度、声音等。这些功能的范围在 Windows 2000 中都得到了扩展。用户也可限制使用一种或几种喜欢的字体。有触觉过敏的用户，可自定义下列辅助功能。

调速模式

调速模式，可能在许多方面对用户有两面的影响。像有癫痫症等触觉过敏的用户，对屏幕刷新速率、闪烁、及闪现的图象，可能会很敏感。Windows 2000 “ 控制面板 ”的设置，能防止默认的动画及视频加载。用户可调整大多数对象闪现的速率，选择一种不会导致发病的频率。用户或管理员可改变“ 插入点指针 ”（有时称为“ 脱字符 ”）的闪烁速率，对屏幕刷新速率过敏的用户，可把该闪烁速率链接到闪现的事件。他们可关闭闪烁或闪现的图象。

声音方案

除了听力损伤的用户及在嘈杂环境工作的用户之外，有触觉过敏的用户也容易受到某些特定声音的影响。Windows 2000 “ 控制面板 ”的设置，能防止默认加载动画及视频。用 Windows 的“ 控制面板 ”，用户可对任何事件指派自定义的声音。自定义声音方案，不管是关闭还是打开声音，也不管是增加还是减少音量，对用户来说，都变得越来越重要，Windows 2000 在很多方面体现出对各种各样残疾及各种各样需求的支持。

颜色和对比度设置

通过“ 控制面板 ”中的“ 辅助功能选项 ”及“ 放大镜 ”，用户可调整颜色及对比度的设置。Windows 2000 新增的一项功能是扩展色谱的颜色方案，用户可自定义它，以适合特殊需求。有关详细内容，请参见有关视力

障碍的下一节。

针对视力障碍用户的选项

对失明或视力低下、色盲、管状视及有其它视力障碍的用户，下列的辅助功能是很有用的。“文本到语音”工具，如“讲述人”；键盘快捷键；“放大镜”；以及象鼠标指针、颜色及对比度方案和其它的用户界面元素等可自定义的功能。

Microsoft “讲述人”

“讲述人”是一个提供最低限度功能的“文本到语音”程序，装在 Windows 2000 美国英语版中。该项新功能要通过 Active Accessibility 工作，读出屏幕上的对象、包括它们的属性以及空间关系。“讲述人”有一些可自定义的选项，让用户能对设备阅读屏幕元素的方式进行自定义。“声音”选项使用户能调整声音的速度、音量及声调。“阅读”选项使用户能选择他们希望设备读出的一些常用字符，如 Delete、Enter、可打印字符或修改符。“鼠标指针”选项能使鼠标指针跟踪屏幕上的活动项目。“在屏幕上通告事件”选项使用户能命令设备在显示以下组件时进行通告：新的窗口、菜单或快捷菜单。对一般视力障碍的用户，“讲述人”提供了最低限度的功能。很多视力很弱的用户，日常工作需要功能更强的工具程序。有关其它基于 Windows 的“文本到语音”工具的更多信息，请参见 Web 资源页的“Microsoft Accessibility”链接，地址是： http://windows.microsoft.com/windows2000/reskit/webresources。

备注 “讲述人”只是一个临时性的辅助工具，不能替代其它软件公司功能完备的“文本到语音”工具。

键盘声音提示

对那些在按 TAB 键时会无意按下 CAPS LOCK 键的用户，“切换键”非常有用；当按了这个键时，“切换键”会即时提供反馈。“切换键”也为那些没有 CAPS LOCK、NUM LOCK 和 SCROLL LOCK 状态指示器的键盘提供了相应功能。

Microsoft “放大镜”

“放大镜”是一功能有限的屏幕放大工具，它能放大 Windows 2000 显示的一部分，让有一定视力障碍的用户更容易阅读屏幕，也可用于图形编辑时，放大屏幕元素。“放大镜”在一个单独的窗口中显示被放大的部分。“放大镜”打开时，被放大的区域只是显示区域，而不是活动区域。对中等视力障碍的用户，“放大镜”提供了最低限度的功能。很多视力弱的用户，日常工作需要功能更强的放大工具程序。有关基于 Windows 的放大镜应用程序的更多信息，请参见 Web 资源页的“Microsoft Accessibility”链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。

备注 “放大镜”不能替代其它软件公司功能完备的放大镜。

字体

要选择字体，用户可单击“控制面板”中“字体”图标，删除不想要的字体。如果他们删除所有的 TrueType 可自定义字体，只留下光栅字体，用户还可以对他们所使用的字号加以限制。TrueType 字体是独立于设备的字体，以外形方式存储，并可放大缩小以显示各种大小尺寸的字符。光栅字体是基于位图的用打印机语言建立的字体。删除字体并非把它们从硬盘上删掉，因此，用户以后可以很容易重新安装这些字体。

备注 在“控制面板”中限制字体，同时也会限制应用程序中可使用的字体。这项操作将影响文档在屏幕及打印中的显示方式；因此，用户对它们施加限制时要非常谨慎。

大小和颜色方案

在“ 辅助功能向导 ”及“ 控制面板 ”中，用户可以调整大多数屏幕元素（如窗口文本、菜单、插入点指针（有时称为“ 脱字符 ”）、鼠标光标、字体及标题栏）的尺寸及颜色。这种功能使系统更易于使用，同时也减少了眼睛的疲劳。在“ 辅助功能向导 ”中，用户可更改图标大小、鼠标指针大小及文本大小。在“ 控制面板 ”中，用户可更改窗口的宽度。通过双击“ 显示 ”图标，然后从“ 外观 ”选项卡中选择喜欢的方案，也能更改 Windows 消息及命令提示窗口中的文字大小。用户可以通过键盘而不是鼠标来调整窗口大小。他们也可在“ 辅助功能向导 ”中，选择“ 我是有视力障碍的人 ”，来调整窗口大小。通过“ 辅助功能向导 ”或“ 控制面板 ”，用户可更改 Windows 消息的字体大小。

在调整颜色设置前，请考虑下列几点：

- 显示大量颜色的设置，需要占用大量的计算机处理器资源。
- High Color 设置包括 65，000 种颜色。True Color 设置包括一千六百万种颜色。
- 监视器及显示适配器决定了屏幕上能显示的最多种颜色的数量。
- 要改变多监视器系统中其它监视器的设置，管理员应选择“ 把我的 Windows 桌面延伸到这个监视器 ” 复选框，来更改其它监视器的设置。他们可为每个已安装的监视器进行颜色设置。

高对比度颜色方案

通过自定义对比度及颜色，可以更轻松地浏览屏幕对象，同时减轻眼睛疲劳。高对比度功能不再是只能通过“ 控制面板 ”激活，它已变成了一个内置的、扩展的配色方案库，能满足那些视力较差的用户对前景色与背景的高对比度的要求。例如，如果用户不能在一个灰色背景上阅读黑色文字，或是图片上的文字，那么他们就能从该功能中受益。激活“ 高对比模式 ”时将自动选择用户喜欢的颜色方案。通过“ 放大镜 ”对话框，用户可反转放大窗口的颜色，或以高对比度显示该屏幕。要“ 高对比模式 ”生效，可能需要花几秒钟的时间。

新鼠标指针

通过“ 辅助功能向导 ”或“ 控制面板 ”自定义的新鼠标指针，用户可以决定哪一种指针的可见性最好。为提高可见性，用户可设置鼠标指针的一些特征，如大小、颜色、速度、动画及可见轨迹。现在指针有 3 种尺寸：大、特大和默认。指针选项包括：白色、黑色及根据屏幕颜色颜色反转的指针。（后面那种指针会变成一种与背景色相对的颜色）。

其它资源

- 有关针对残疾用户的辅助功能的更多信息，包括技术支持、文档及相关的组织机构，请参见 Web 资源页的“ Microsoft Accessibility ”链接，地址是：http://windows.microsoft.com/windows2000/reskit/webresources。
- 有关键盘快捷键的更多信息（包括辅助功能键盘快捷键的详细列表），请参见 Microsoft Corporation， 1998，Redmond，WA: Microsoft Press. 出版的 *Microsoft Windows 98 Resource Kit* 中的“ Appendix H – Accessibility ”。

  有关残疾用户辅助功能的更多信息及辅助功能编目，可按以下方式给 Microsoft 打电话或写信：

  - Microsoft 销售信息中心电话：: 1 + (800) 426-9400
  - Microsoft 销售传真服务线路电话，以接收传真反馈文档： 1 +(800) 727-3351

- Microsoft 销售信息中心的通信联系地址： One Microsoft Way, Redmond, WA 98052-6393。

Windows 2000 Server 部署指南术语表

.adm

管理模板文件的文件扩展名。

.msi

Windows 安装服务软件包文件的文件扩展名。

A

access control / 访问控制

Windows NT 和 Windows 2000 中的安全机制，它决定安全负责者能够使用哪些对象以及如何使用它们。另请参见“ 授权 ”、“ 安全负责者 ”。

access control entry (ACE) / 访问控制项

访问控制列表 (ACL) 中的一项，包含一个安全 ID (SID) 和一组访问权限。拥有相匹配的安全 ID 的进程将被允许访问、禁止访问，或经授权后访问。

access control list (ACL) / 访问控制列表

安全描述符的一部分，它列举了应用于对象的保护措施。对象的所有者具有对该对象的任意访问控制，他可以改变 ACL 以允许或禁止他人访问该对象。ACL 由访问控制项 (ACE) 组成。Windows NT 或 Windows 2000 中对象的每个安全描述符都包含四个安全组件：创建者（所有者）；组，为与 POSIX 相符合，并与用户管理器中单个用户对象的“ 主要组 ”设置相关联；任意访问控制列表（DACL，通常简称为 ACL），决定该对象的权限；以及系统访问控制列表（SACL），决定审核。另请参见“ 任意访问控制列表 ”。

access token / 访问令牌

该对象包含登录会话所需的安全信息。当用户登录时 Windows 2000 将创建一个访问令牌，该用户执行的每个进程都拥有该令牌的一个副本。令牌标识的是用户、用户组以及用户特权。系统通过令牌控制对可保护对象的访问，并控制用户在本地计算机上执行各种与系统相关的操作的能力。访问令牌分两种：主令牌和模拟令牌。另请参见“ 主令牌 ”、“ 模拟令牌 ”、“ 特权 ”、“ 进程 ”以及“ 安全标识符 ”。

accessibility / 辅助功能

系统组合使用硬件或软件，通过可定制的用户界面、替代输入输出方法以及放大屏幕组件等手段，使有感知、听觉、身体或视觉障碍的人也可以使用计算机的性质。

accessibility wizard / 辅助功能向导

一种交互式的工具，它通过指定障碍类型（而非改变数值）简化设置常用辅助功能的工作。

account domain / 帐户域

保存用户帐户数据的 Windows NT 域，也称主域。

account lockout / 帐户锁定

一种 Windows 2000 安全功能。若在一定时间内发生多次登录操作失败，则根据安全策略锁定的设置，锁定

用户帐户。（无法登录被锁定的帐户。）

Active Directory

Windows 2000 Server 包含的目录服务。它保存网络中的对象信息，并使用户和网络管理员可以使用该信息。Active Directory 允许网络用户以一次登录，访问网络中任何位置允许访问的资源。它为网络管理员提供了直观的网络层次视图，和管理所有网络对象的切入点。另请参见“目录”、“目录服务”。

Active Directory Connector (ADC) / Active Directory 连接器

Windows 2000 Server、Windows 2000 Advanced Server 以及 Windows 2000 Enterprise Server 的同步代理，它可以自动保持两个目录之间目录信息的一致性。如果没有 ADC，您将不得不手动输入新数据，更新信息到所有的目录服务。

Active Directory Installation wizard / Active Directory 安装向导

一种 Windows 2000 Server 工具，它允许在安装时进行以下操作：安装 Active Directory、在目录林中创建目录树、复制一个已存在的域、安装 Kerberos 身份验证软件以及将服务器提升为域控制器。

Active Directory replication / Active Directory 复制

由目录复制程序服务执行的复制，它提供在域控制器之间目录分区的多主体复制。所谓“多主体”指每个域控制器中的目录分区副本均为可写。复制服务将更改的内容从给定的目录分区副本复制到拥有同样目录分区副本的所有其他域控制器。另请参见“目录分区”、“文件复制服务”。

Active Directory Service Interfaces (ADSI) / Active Directory 服务接口

一种目录服务模型以及一组 COM 接口。ADSI 使得 Windows 95、Windows 98、Windows NT 以及 Windows 2000 应用程序可以访问包括 Active Directory 在内的多个网络目录服务。它以软件开发工具包 (SDK) 的形式提供。

active partition / 活动分区

计算机从该分区启动。活动分区必须是基本磁盘上的一个主分区。如果单独使用 Windows 2000，活动分区可以与系统分区相同。如果 Windows 2000 与 Windows 98 或更早的产品、或 MS-DOS 一起使用，则活动分区必须包含所有操作系统的启动文件。

active/active / 主动/主动

应用程序的一种群集配置，在此配置下应用程序在所有的节点同时运行。另请参见“主动/被动”。

active/passive / 主动/被动

应用程序的一种群集配置，在此配置下任一时刻应用程序只能在一个节点运行。另请参见“主动/主动”。

ActiveX

该套技术使得软件组件可以在联网环境下交互，而不管创建组件时使用何种语言。

address / 地址

在系统管理服务器中，地址用于连接站点和站点系统。发件人使用地址将指令和数据发送到其他站点。

address classes / 地址类别

参见“ 网际地址类别 ”。

address pool / 地址池

一定范围内的一组 IP 地址。地址归入地址池后可以由 DHCP 服务器动态地分配给 DHCP 客户。

Address Resolution Protocol (ARP) / 地址解析协议

TCP/IP 中的一种协议，它通过向本地网络发布有限广播，解析逻辑分配的 IP 地址。各 IP 网络主机设备的 IP 地址是在软件中被指派到其物理硬件或媒体访问控制层地址的。对 ATM 而言，ARP 协议以两种不同方式使用。对 CLIP 而言，ARP 用于将 IP 地址解析为 ATM 硬件地址。在 ATM 局域网仿真中，ARP 用于将 Ethernet/802.3 或令牌环地址解析为 ATM 硬件地址。另请参见“ 媒体访问控制 ”、TCP/IP。

administrative templates (.adm files) / 管理模板（.adm 文件）

管理模板（.adm 文件）是一种 ASCII 文件，组策略利用它可以生成可由管理员设置的用户界面设置。

admission control / 许可控制

此服务用于在共享网段上管理控制网络资源。

Advanced Configuration and Power Interface (ACPI) / 高级配置和电源接口

一种开放式工业规范，它规定了各种移动、桌面及服务器计算机和外设的电源管理。ACPI 是当今工业创新的基础，它允许系统制造商发售由键盘触发的计算机。ACPI 设计是充分利用 Windows 2000 的电源管理和即插即用功能之根本。请核查制造商的文档以验证计算机是否是 ACPI 兼容的。另请参见“ 即插即用“ 。

advertise / 公布

在系统管理服务器中，使程序对一个集合（组）中的成员可用。

advertisement / 公布

在系统管理服务器中，由站点服务器向客户访问点（CAP）发送的说明客户可以使用一个软件分发程序的通知。

agent / 代理

一个运行于由简单网络管理协议（SNMP）管理的设备上的应用程序。代理应用程序是管理活动的对象。运行 SNMP 代理软件的计算机有时也称为代理。

algorithm / 算法

解决问题的法则或步骤。网际协议安全措施用基于密码的算法进行数据加密。

alternative input devices / 替代输入设备

该输入设备由那些不能使用鼠标、键盘等标准输入设备的用户使用。

answer file / 应答文件

无人职守安装 Windows 2000 时，该文本文件将提供自动输入。该输入包含具体安装时，安装程序所要求的应答参数。在某些情况下，您可以使用该文本文件为向导提供输入。例如 Active Directory 安装向导，它通过安装程序将 Active Directory 添加到 Windows 2000 Server。安装程序默认的应答文件为 Unattend.txt。

AppleTalk

Apple 计算机网络体系结构和网络协议。拥有 Macintosh 客户和运行具有 Macintosh 服务功能的 Windows 2000 Server 计算机的网络是一个 AppleTalk 网络。

AppleTalk Protocol / AppleTalk 协议

AppleTalk 网络体系结构所基于的网络协议组。运行 Windows 2000 Server 的计算机只有安装 AppleTalk 协议栈后，才能够与 Macintosh 客户连接。另请参见 AppleTalk。

application assignment / 应用程序指派

使用软件安装（组策略的一种扩展）向用户组指派程序的进程。用户登录时，该程序出现在其桌面上。

application programming interface (API) / 应用程序接口

一组例程，应用程序通过它们请求并执行由计算机操作系统执行的低层服务。这些例程通常执行诸如管理文件和显示信息等维护任务。

area / 区域

OSPF 自治系统中的一组相连网络。OSPF 区域将减小链接状态数据库的大小，并提供总结路由的能力。另请参见“自治系统”、“链接状态数据库”。

area border router (ABR) / 区域边界路由器

隶属于多个区域的路由器。区域边界路由器为每个区域维护单独的链接状态数据库。另请参见“链接状态数据库”。

ARP Cache / ARP 高速缓存

一张 IP 地址及其相应媒体访问控制地址的列表。每个接口各有单独的 ARP 高速缓存。

assigning / 指派

在系统管理服务器中，将程序部署给必须接受该程序的集合（组）的成员。

Asynchronous Transfer Mode (ATM) / 异步传输模式

一种面向连接的高速协议，用于传输多种网络通信业务。

attribute (object) / 属性（对象）

Active Directory 中对象的单项属性。对象由属性值描述。对于每种对象类别，架构定义了该类别的实例必须具有哪些属性，以及可能具有的附加属性。

attributes (file) / 属性（文件）

该信息说明一个文件是否为只读、隐藏、可存档（备份）、压缩或加密，以及该文件内容是否应该编制索引以便快速查找文件。

auditing / 审核

通过在服务器或工作站的安全日志中记录选定类型的事件，跟踪用户活动。

augmentative communication devices / 增强式通信设备

可以帮助残疾用户通过辅助技术控制计算机的附加软件和硬件。例如语音识别系统和屏幕阅读器。

authentication / 身份验证

网络访问时系统验证用户登录信息的过程。它将用户名和密码与一个已验证了的列表进行比较。如果系统检测到匹配项，则按照该用户权限列表中指定的范围授予访问权。如果用户登录到运行 Windows 2000 Professional 的计算机上的帐户，则身份验证由客户机执行。当用户登录到一个 Windows Server 域时，身份验证可以由该域的任何服务器执行。另请参见“ 服务器 ”、“ 信任关系 ”。

authentication / 身份验证

通过确保每台计算机的真正标识，验证消息来源和完整性的 IPSec 进程。如果没有强加密身份验证，未知计算机和它所发送的任何数据都是值得怀疑的。IPSec 提供多种身份验证方法，以确保与运行 Windows 早期版本的老系统、非基于Windows 的系统以及共享计算机的兼容性。

authoritative / 权威

对域名系统（DNS）来说，DNS 服务器在注册和解析 DNS 域名时对区域的使用。当 DNS 服务器被配置为主持一个区域时，它就是该区域内的名称权威。对 DNS 服务器授权将根据存储在区域中的信息进行。另请参见“ 区域 ”。

authoritative restore / 授权还原

在备份程序中对 Windows 2000 域控制器进行的一种还原操作，此操作中被还原目录中的对象将视为具有权威，替换（通过复制）这些对象的所有现存副本。授权还原只适用于复制的系统状态数据，例如 Active Directory 数据和文件复制服务数据。授权还原由 Ntdsutil.exe 工具执行。另请参见“ 未授权的还原 ”、“ 系统状态 ”。

authorization / 授权

在远程访问或请求拨号型连接中，验证连接尝试是否允许。授权在成功的身份验证之后发生。

automated installation / 自动安装

使用诸如远程安装服务、引导 CD 及 Sysprep 等一种或多种方法，执行无人职守安装。

Automatic Private IP Addressing (APIPA) / 自动专用 IP 寻址

Windows 2000 TCP/IP 的一项功能，当 TCP/IP 协议被配置为动态寻址和动态主机配置时，它自动在 169.254.0.1 和 169.254.255.254 之间配置一个唯一的 IP 地址，并设子网掩码为 255.255.0.0。

autonomous system (AS) / 自治系统

使用公共路由协议交换路由信息的路由器组。

availability / 可用性

计算机及其程序容错性能的量度。可用性高的计算机每周 7 天每天 24 小时运行。另请参见“ 容错 ”。

B

backbone / 基干

OSPF 中一个为其他所有 OSPF 区域所公用的区域，它作为区域间通信和在区域间传播路由信息的传输区域使用。基干必须相互连接。另请参见“ 开放式最短路径优先（OSPF） ”。

backup domain controller / 备份域控制器

在 Windows NT Server 4.0 或更早版本中，一台运行 Windows NT Server，并负责接收域的目录数据库（包含该域所有帐户和安全策略信息）副本的计算机。该副本周期性地同主域控制器上的主控数据库取得同步。备份域控制器也验证用户登录信息，并在需要时可以被提升为主域控制器。一个域中可以存在多个备份域控制器。当 Windows 2000 域被配置为混合模式时，Windows NT 3.51 及 4.0 的备份域控制器也可以加入其中。另请参见“ 混合模式 ”、“ 主域控制器 ”。

backup operator / 备份操作员

一种本地或全局的组类型，该组具有备份、还原文件及文件夹所需的用户权利。备份操作员组的成员可以备份、还原文件及文件夹，而不管所有权、访问权限、加密、或审核设置如何。另请参见“ 审核 ”、“ 全局组 ”、“ 本地组 ”、“ 用户权限 ”。

backup set / 备份集

已被备份，并存放于文件或磁带上的文件、文件夹和其他数据的集合。

bandwidth / 带宽

事实上通信中在给定范围内最高频率和最低频率之间的差额。例如，一条电话线路提供 3000 Hz 的带宽，即其所能承载的最低频率（300 Hz）和最高频率（3300 Hz）之间的差额。在计算机网络中，较宽的带宽意味着更快的数据传送能力。带宽以每秒位数 (bps) 为单位表示。

Bandwidth Allocation Protocol (BAP) / 带宽分配协议

一种 PPP 控制协议，用于多重处理连接，以动态地添加和删除链接。

basic disk / 基本磁盘

包含主分区或扩展分区的物理磁盘，其逻辑驱动器由 Windows 2000 和所有其他版本 Windows NT 所使用。基本磁盘也可以包含通过 Windows NT 4.0 或更早期版本创建的卷集、带区集、镜像集或 RAID-5 集。既然使用兼容的文件格式，MS-DOS、Windows 95、Windows 98以及所有版本的 Windows NT 就都可以访问基本磁盘。

basic volume / 基本卷

基本磁盘上的一个卷。基本卷包含主分区、扩展分区中的逻辑驱动器以及通过 Windows NT 4.0 或更早期版本创建的卷集、带区集、镜像集或 RAID-5 集。只有基本磁盘才能包含基本卷。基本卷和动态卷不能共存于同一只磁盘。

binary / 二进制

一种基数为 2 的数字系统，以数字 0 和 1 的组合表示数值。

bindery / 平构数据库

Novell NetWare 2.x 和 3.x 中的一个数据库，它包含用户和组的单位及安全信息。

binding / 绑定

将软件组件和网络层次链接到一起的进程。在安装网络组件后，组件的绑定关系及依存关系亦随之建立。绑定允许组件之间相互通信。

bit / 位

计算机处理的最小信息单位。一个位表示二进制数中的一个 1 或 0，或者是真或假的逻辑条件。一个 8 位组构成一个字节，字节可以代表许多类型的信息，例如字母表中的一个字母、一个十进制数字、或其他字符。位又称为二进制数字。

bits per second (bps) / 每秒位数

每秒传输的位数，用以度量调制解调器等设备的数据传送速度。一个字符由 8 个位组成。在异步通讯中，每个字符前面有一个起始位，并以一个停止位终止。因此，传输一个字符要传输 10 个位。如果一个调制解调器以每秒 2400 位 (2400 bps) 的速度通信，则每秒传送 240 个字符。

block policy option / 阻止策略选项

一个阻止由高层 Active Directory 容器指定的组策略应用于计算机或用户的选项。

boot / 启动

启动或复位计算机。当第一次加电或复位时，计算机执行装入并启动操作系统的软件，以备使用。

bootable CD-ROM / 引导 CD-ROM

从 CD-ROM 上运行安装程序的一种自动安装方法。此方法对于远程站点上链接较慢而且没有本地 IT 部门的计算机有益。另请参见“自动安装”。

bootstrap protocol (BOOTP) / 引导协议

一组规则或标准，使得计算机能够相互连接，主要用于在 TCP/IP 网络中配置无盘工作站。该协议由 RFC 951 和 1542 定义。DHCP 是使用该协议的一种启动配置协议。

bottleneck / 瓶颈

一种使整个系统性能低下的情况，通常与硬件资源有关。

BounceKeys / 回弹键

一种键盘筛选器，用于帮助按下或释放按键时手指在其上跳动的用户。

bridgehead server / 桥头服务器

一种在连接协议的每个端点接收和转发电子邮件通信的服务器，执行的任务类似于网关。

broadcast / 广播

以给定网络上所有主机为信宿的地址。另请参见“广播网络”。

broadcast and unknown server (BUS) / 广播与未知服务器

仿真局域网络 (ELAN) 上的一种多播服务，它将转发来自 LAN 仿真客户的广播、多播以及初始单播通信数据。另请参见“仿真局域网络 (ELAN)”。

broadcast network / 广播网

支持两个以上关联路由器并具有将单条物理消息寻址到所有关联的路由器（广播）之能力的网络。以太网是广播网络的一个实例。

browse list / 浏览列表

任何可以浏览的项目列表，比如说一个网络上的服务器列表或在填加打印机向导中列出的打印机列表。

browser / 浏览器

在 Internet 或 intranet 上导航和访问信息的一种客户工具。在 Windows 网络上下文环境中，“ 浏览器 ”也可以指计算机浏览器服务，一种维护一个网络或网络的一部分上的最新的计算机列表的服务。

这种服务还应应用程序请求向其提供列表。当用户试图连接到域中的某资源时，该域的浏览器会被联系以提供一个可用资源的列表。

buffer / 缓冲区

一个内存区域，用于在数据使用前暂存之。

bulk encryption / 批量加密

一个出于保密目的而对大量的数据，比如说文件、电子邮件消息或联机通信会话，加密的过程。这通常用对称密钥算法来完成。另请参见“ 加密 ”、“ 对称密钥加密 ”。

BUS

参见“ 广播与未名服务器 “ 。

bus / 总线

用于计算机系统组件之间的数据传送的一种通信线路。总线实质上是一条允许系统不同部分共享数据的信息公路。

C

cable modem / 电缆调制解调器

一种提供带宽在 10 到 30 Mbps 范围内的宽带 Internet 接入的调制解调器。

cache / 高速缓存

对 DNS 和 WINS 而言，是指一个保存最近解析的远程主机名称的资源记录的本地信息存储区。典型地，高速缓存是在计算机查询和解析名称时建立起来的 ;它有助于减少解析被查询名称所需要的时间。另请参见“ 高速缓存文件 ”、“ 名称服务 ”、“ 资源记录 ”。

cache file / 高速缓存文件

域名系统（DNS）服务器在系统启动时用来预加载其名称高速缓存的一个文件。也称为“ 根线索 ”文件，这是因为该文件中保存的资源记录被 DNS 服务用来协助定位根服务器，而根服务器则提供获得远程名称所需的权威服务器的参照信息。对 Windows DNS 服务器而言，高速缓存文件被命名为 Cache.dns 并位于 %Systemroot%\System32\Dns 文件夹中。另请参见“ 权威 ”“ 高速缓存 ”、systemroot。

caching / 缓存

对 DNS 而言，通常是指 DNS 服务器保存在名称查询处理和解析中所获得的域名称空间信息的服务器方能力。

在 Windows 2000 中，缓存也可被 DNS 客户服务（解析器）用作 DNS 客户维持在最近查询中所获得的名称信息的一个高速缓存的一种方法。另请参见“ 缓存解析器 ”。

caching resolver / 缓存解析器

对 Windows 2000 而言，是指执行对最近获得的 DNS 域名信息的缓存的一种客户方域名系统（DNS）名称解析服务。缓存解析器服务提供了在系统范围内对支持 DNS 的程序的访问，以获得在处理名称查询时从 DNS 服务器所获得的资源记录。处于该高速缓存内的数据只用于一段有限的时间，它根据其活动生存时间 （TTL）值而老化。您既可以对每条资源记录（RR）分别设置 TTL 值，也可以对区域默认在 SOA RR 中所设置的最小值。另请参见“ 高速缓存 ”、“ 缓存 ”、“ 过期间隔 ”、“ 最小 TTL ”、“ 资源记录 ”、“ 生存时间(TTL) ”。

Call Manager / 呼叫管理器

一个软件组件，它建立、维护和终止两台计算机之间的连接。

central site / 中央站点

在 Systems Management Server （系统管理服务器）中，是指位于 Systems Management Server （系统管理服务器）层次顶端的主站点，在此 Systems Management Server （系统管理服务器）系统中的所有其他站点都向它报告其清单和事件。

certificate / 证书

用于在不安全网络，比如说 Internet，上进行身份验证和数据的安全交换的一个文件。证书安全地将一个公共密钥绑定到保存其相应私钥的实体。证书由其证书颁发机构数字签名，并可用于用户、计算机、或服务。

certificate revocation list (CRL) / 证书吊销列表

由证书颁发机构维护和发行的一个文挡，它列出了被吊销的证书。为确保其完整性，CRL 是用 CA 的私钥签名的。另请参见“ 证书 ”、“ 证书颁发机构 ”。

certificate services / 证书服务

向某特定 CA 颁发证书的 Windows 2000 服务。它为企业提供了颁发和管理证书的可定制服务。另请参见“ 证书 ”、“ 证书颁发机构 ”。

certificate stores / 证书存储区

Windows 2000 在逻辑存储区和物理存储区内保存公钥对象，例如证书和证书吊销列表。逻辑存储区为用户、计算机、及服务对公钥对象进行分组。物理存储区是本地计算机注册表中（或者对某些用户证书而言是在 Active Directory 中）实际存储公钥的地方。逻辑存储区包含指向物理存储区内的公钥对象的指针。用户、计算机、以及服务共享许多公钥对象，因此，逻辑存储区使得它们可以共享公钥对象而不需要为每个用户、计算机、或服务保存对象的副本。

certificate template / 证书模板

一种 Windows 2000 构造，它根据想要的用途勾画证书的轮廓（即预先指定格式和内容）。当向 Windows 2000 证书颁发机构(CA)请求证书时，根据其访问权限，请求者将可以从多种证书类型中进行选择，比如说“ 用户 ”和“ 代码签名 ”，而这些证书类型则是基于证书模板的。另请参见“ 证书 ”、“ 证书颁发机构 ”。

certificate trust list (CTL) / 证书信任列表

一个签名的根证书颁发机构证书，它被管理员视为可以放心地用于指定的目的（比如说客户身份验证或安全电子邮件）。另请参见“ 证书 ”、“ 证书颁发机构 ”、“ 根证书 ”、“ 根证书颁发机构 ”。

certification authority (CA) / 证书颁发机构

一个实体，负责建立属于用户的（终端实体）或其他证书颁发机构的公钥并保证其真实性。证书颁发机构的活动可以包括通过签名的证书将公钥绑定到特定的名称、管理证书的序列号和吊销证书。另请参见“ 证书 ”、“ 公钥 ”。

certification hierarchy / 证书等级

一种证书信任模型，在其中证书路径是通过在证书颁发机构之间建立父子关系来创建的。另请参见“ 证书颁发机构 ”、“ 证书路径 ”。

certification path / 证书路径

证书等级中从一个证书到根证书颁发机构的一条不间断信任链。另请参见“ 证书等级 ”、“ 证书 ”。

Challenge Handshake Authentication Protocol (CHAP) / 挑战握手身份验证协议

一种 RFC 1994 中的 PPP 连接的挑战-响应身份验证协议，使用工业标准消息摘要 5（MD5）单向加密方案来散列化对远程访问服务器颁发的挑战的响应。

change log / 更改日志

参见“ 定额日志 ”。

child domain / 子域

对 DNS 和 Active Directory 而言，是指在名称空间树中直接位于另一个域名(父域)下的 DNS 域。例如，"example.reskit.com" 是

父域 "reskit.com." 的一个子域。child domain 又称为 subdomain（子域）。另请参见“ 父域 ”、“ 域 ”、“ 目录分区 ”。

child object / 子对象

处于另一个对象中的对象。子对象意味着某种关系。例如，文件是处于文件夹中的一个子对象，而文件夹则是父对象。另请参见“ 对象 ”、“ 父对象 ”。

cipher / 密码

构成一条隐藏消息的方法。密码用来将一条称为明文（有时也称明码）的可读消息转换为一条称为暗记文的不可读的、扰码的、或者是隐藏的消息。只有拥有机密的解码密钥的人才能将暗记文转换回原来的明文。另请参见“ 暗记文 ”、“ 明文 ”、“ 加密 ”。

ciphertext / 暗记文

用加密密钥加了密的文本。对任何没有解密密钥的人来说，暗记文都毫无意义。另请参见“ 解密 ”、“ 加密 ”、“ 加密密钥 ”、“ 明文 ”。

Class A IP address / A 类 IP 地址

1.0.0.1 到 126.255.255.254 之间的一个单播 IP 地址。其第一个八位组指明网络，后面的三个八位组指明该网络上的主机。另请参见“ B 类 IP 地址 ”、“ C 类 IP 地址 ”、“ IP 地址 ”。

Class B IP address / B 类 IP 地址

128,0.0.1 到 191.255.255.254 之间的一个单播 IP 地址。头两个八位组表示网络，后两个八位组表示该网络上的主机另请参见“A 类 IP 地址”、“C 类 IP 地址”、“IP 地址”。

Class C IP address / C 类 IP 地址

192,0.0.1 到 223.255.255.254 之间的一个单播 IP 地址。其前三个八位组指明网络，最后一个八位组指明该网络上的主机。网络负载平衡为 C 类 IP 地址提供了可选的支持（在支持单一 IP 地址的基础上），以适应在客户站点使用多代理服务器的客户。另请参见“A 类 IP 地址”、“B 类 IP 地址”、“IP 地址”。

Class D IP address / D 类 IP 地址

这种网际地址类别是为 IP 多播地址而设计的。D 类 IP 地址及网络的第一个八位组的值在 224 到 239 之间。

classless interdomain routing (CIDR) / 无类别域间路由

一种不根据原始网际地址类别的公用 IP 地址分配方法。无类别域间路由（CIDR）是开发来协助防止公共 IP 地址耗尽和最小化 Internet 路由表大小的。

clean installation / 清洁安装

在计算机硬盘的一个清洁分区或空分区安装操作系统的过程。

client / 客户

任何连到其他计算机或程序的，或请求其他计算机或程序的服务的计算机或程序。另请参见“服务器”。

client access point / 客户访问点

Systems Management Server（系统管理服务器）中，提供一组共享目录和文件、创造了一个站点服务器和客户计算机之间的公共通信点的站点系统。

client request / 客户请求

从客户计算机到服务器计算机（或者，对网络负载平衡为到一群计算机）的服务请求。网络负载平衡根据系统管理员负载平衡策略将每条客户请求转发到群集内一特定的主机。请参见“客户”、“群集”、“主机”、“服务器”。

Client Service for Netware / NetWare 客户服务

Windows 2000 Professional 包含的一种服务，允许客户计算机直接连接运行 NetWare 2.*x*、3.*x*、4.*x*、或 5.*x* 服务器软件的计算机上的资源。

client-side extensions / 客户方扩展

组策略组件，在某些情况下，负责在客户计算机上实现组策略。

ClonePrincipal

一种允许用户以增量方式迁移到 Windows 2000 环境而不影响现存的 Windows NT 产品环境的工具。

closed captioning / 已关闭标题

只能在一台特殊装备的接收机上才能看到的音频或图形媒体的替代表示，通常是文本。

cluster / 群集

共同工作以提供一项服务的一组计算机。群集的使用既增强了服务的可用性又增强了提供该服务的操作系统的可扩展性。网络负载平衡为群集多台运行 Windows 2000 Advanced Server、在 Internet 和专用 intranet 上提供网络化服务的计算机提供了一种软件解决方案。另请参见“ 可用性 ”、“ 可扩展性 ”。

Cluster Administrator / 群集管理器

一个用于配置一个群集及其节点、组、以及资源的应用程序 (Cluadmin.exe)。群集管理器可以运行于受信域中任何成员上，而不管该计算机是否是一个群集节点。另请参见“ 群集 ”、“ 群集管理器扩展 ”、Cluster.exe、“ 节点 ”、“ 资源 ”。

Cluster Administrator extension / 群集管理器扩展

一个使得群集管理器能管理自定义资源类型的动态链接库 (DLL)。群集管理器扩展使用群集管理器扩展 API。另请参见“ 群集 ”、“ 群集管理器 ”、“ 资源 ”。

cluster API / 群集 API

由群集软件实现的一组功能，由支持群集的客户或服务器应用程序、群集管理应用程序或资源 DLL 所使用。群集 API 用于管理群集、群集对象、以及群集数据库。另请参见“ 群集 ”、“ 支持群集的应用程序 ”、“ 动态链接库 ”、“ 节点 ”、“ 资源 ”、“ 资源 DLL ”。

Cluster service / 群集服务

Clussvc.exe，Windows Clustering 组件中创建服务器群集的主可执行程序，控制其操作的各个方面、并管理群集数据库。服务器群集中的各个节点都运行群集服务的一个实例。

cluster-aware / 支持群集的

运行于服务器群集节点的应用程序或服务的一种分类，它被当作一种群集资源来管理，并被设计为支持服务器群集环境并与之交互。

cluster-aware application / 支持群集的应用程序

运行于服务器群集节点的并被当作一种群集资源来管理的一种应用程序或服务。支持群集的应用程序使用群集 API 来从服务器群集接收状态或通知信息。另请参见“ 群集 API ”、“ 不支持群集的应用程序 ”、“ 节点 ”。

cluster-unaware application / 不支持群集的应用程序

服务器群集中运行于一个节点并被作为一个群集资源来管理、但不支持群集 API、因而也就对其环境不具有固有知识的一种应用程序。不支持群集的应用程序不管

是运行于服务器群集中的一个节点还是非群集系统，其行为都是一样的。另请参见“ 支持群集的应用程序 ”、“ 节点 ”。

Cluster.exe

在 Windows 2000 命令提示符下使用群集管理器管理群集的一种替换选项。可以从命令脚本中调用 Cluster.exe 以自动执行许多群集管理任务。另请参见“ 群集管理器 ”。

code signing / 代码签名

对软件代码进行数字签名以确保其一致性和提供对其来源的担保。

cognitive disabilities / 感知障碍

由于知觉异常、记忆丢失而造成的损害，以及诸如诵读困难和 Down 综合症等学习和发展障碍。

collection / 集合

在 Systems Management Server（系统管理服务器）中是指由成员规则所定义的一组资源。集合用于为远程工具会话分发软件、查看客户机上的清单、以及访问客户。

common gateway interface (CGI) / 公共网关接口

用于启动软件服务的一个服务器方接口。说明 Web 服务器如何与在同一台计算机上的软件之间通信的一组接口。任何软件，只要它按照 CGI 标准来处理输入输出，就都是 CGI 程序。

Common Internet File System (CIFS) / 公用 Internet 文件系统

一种协议及相应 API，由应用程序用来请求高层应用程序服务。CIFS 原为 SMB（服务器消息块）。

Component Object Model (COM) / 组件对象模型

一种为提高软件互操作性而设计的基于对象的编程模型，它允许两个或两个以上的应用程序或组件能很容易地协作。即使这些应用程序或组件是由其他供应商或用不同语言写的，或者是运行于操作系统不一样的不同计算机上，都不例外。COM 是更大范围的技术赖以建立的基础。Microsoft 对象链接与嵌入 (OLE) 技术和 ActiveX 都是建立在 COM 之上的。

Component Server / 组件服务器

为运行诸如应用程序负载平衡、事务服务及应用程序管理之类的组件服务提供平台的服务器。

computer account objects / 计算机帐户对象

Windows NT Server 4.0 或 Windows 2000 Server 中用来标识某一特定计算机帐户的对象。

computer name / 计算机名

一个最大长度不超过 15 个大写字母的在网络中唯一标识一台计算机的名称，。该名称不能与网络中的任何其他计算机或域的名称相同。

confidentiality / 保密

一种 Internet 协议安全服务，通过加密数据来确保消息只透露给预定接收者。

connection agreement / 连接协议

ADC UI 中的一个可配置的部分，保存诸如以下的信息：为取得同步而联系的服务器的名称、要同步的对象类型、目标容器、以及同步计划。另请参见“ Active Directory 连接器 (ADC)”。

connection-oriented / 面向连接的

一种网络协议类型，要求在通过网络通信前在发送方和接收方之间建立一条端到端的虚连接。

console tree / 控制台树

Microsoft 管理控制台 (MMC) 中显示层次化的名称空间的树状视图窗格。默认情况下它是控制台窗口的左窗格，但也可以隐藏。控制台树中的条目（例如 Web 页、文件夹、以及控件）及其层次结构决定控制台的管理能力。另请参见“ Microsoft 管理控制台 (MMC) ”、“ 名称空间 ”。

consoles / 控制台

用来在 Microsoft 管理控制台 (MMC) 中拥有管理工具的框架。控制台由控制台树中的项目定义，控制台树可能包含文件夹或其他容器、万维网页面、及其他管理项目。控制台有可以为控制台树和管理属性、服务、及控制台树项目所激发的事件提供视图的窗口。

container object / 容器对象

可以在逻辑上拥有其他对象的一个对象。例如，文件夹是一个容器对象。另请参见“ 非容器对象 ”、“ 对象 ”。

convergence / 收敛

网络中发生变化后系统稳定的过程。对路由来说，如果一个路由器变得不稳定，则各路由器通过互联网发送更新消息，重新建立关于首选路由的信息。对网络负载平衡来说，是指主机交换消息以确定该群集的一个新的一致的状态以及以最高主机优先级来选出称为默认主机的主机的一个过程。在收敛过程中，为共同处理特定 TCP 或 UDP 端口网络业务流的主机确定一个新的负载分配。另请参见“ 群集 ”、“ 默认主机 ”、“ 主机 ”、“ 用户数据报协议 (UDP) ”。

cost / 开销

配置于 OSPF 路由器说明使用某链接的倾向的一个没有单位的指标。

crypto-accelerator board / 加密加速板

一种通过将操作下载到电路板上的一个特殊处理器进行来加速加密操作的硬件设备。

CryptoAPI (CAPI)

作为 Windows 2000 的一部分提供的一种应用程序编程接口 (API)。CryptoAPI 提供了一组功能，允许应用程序在对私钥提供保护的同时以一种灵活的方式对数据进行加密或数字签名。实际的加密操作由称为加密服务提供程序 (CSP) 的独立模块进行。另请参见 “ 加密服务提供程序 ”、“ 私钥 ”。

cryptographic service provider (CSP) / 加密服务提供程序

执行诸如机密密钥交换、数据的数字签名、以及公钥身份验证之类的加密操作的一个独立软件模块。任何 Windows 2000 服务或应用程序都可以向 CSP 请求加密操作。另请参见“ CryptoAPI ”。

cryptography / 加密

信息安全的艺术与科学。它提供了四个基本的信息安全功能：保密、完整性、身份验证、以及认可。另请参见“ 保密 ”、“ 完整性 ”、“ 身份验证 ”、“ 认可 ”。

custom subnet mask / 自定义子网掩码

一个不是基于网际地址类别的子网掩码。子网化时常常用到自定义子网掩码。

D

datagram / 数据报

发往另一个网络信宿的未答复的数据包。信宿可以是局域网（LAN）上可直达的另一个设备，也可以是可使用经由数据包交换网络的有路由的传输达到的远程信宿。

DCOM

另请参见“分布式组件对象模型”。

DCOM Configuration tool / DCOM 配置工具

一种 Windows NT Server 工具，可用来为网络上的 DCOM 通信配置 32 位应用程序。另请参见 DCOM。

decryption / 解密

将暗记文转换为明文使加密数据从新变得可读的过程。另请参见“暗记文”、“加密”、“明文”。

default gateway / 默认网关

TCP/IP 协议的一个配置项目，是直接可达的 IP 路由器的 IP 地址。配置一个默认网关则会在 IP 路由表中创建一条默认路由。

default host / 默认主机

具有最高主机优先级的主机，对其没有 drainstop 命令在处理。收敛后，默认主机处理对没有被端口规则所覆盖的 TCP 和 UDP 端口的所有网络业务流。另请参见“收敛”、drainstop、“主机优先级”、“端口规则”、“用户数据报协议”。

default network / 默认网络

Macintosh 环境下在其中服务器进程作为节点存在并且服务器对用户可见的物理网络。服务器的默认网络必须是服务器所属的一个网络。只有 AppleTalk Phase 2 Internet 中的服务器才有默认网络。

default route / 默认路由

当路由表中找不到对信宿的其他路由时所使用的路由。例如，如果一个路由器或终端系统找不到信宿的网络路由或主机路由，则使用默认路由。默认路由用于简化终端系统或路由器的配置。对 IP 路由表而言，默认路由即是那条网络信宿为 0.0.0.0、信宿为 0.0.0.0 的路由。

default subnet mask / 默认子网掩码

一个用于基于网际地址类别的网络的子网掩码。A 类的子网掩码为 255.0.0.0。B 类的子网掩码为 255.255.0.0。C 类的子网掩码为 255.255.255.0。

defragmentation / 碎片整理

重写文件某些部分到硬盘上的连续扇区以提高访问与恢复速度的过程。文件更新时，计算机往往将更新写到硬盘上最大的连续空间，而这往往和该文件的其他部分不在同一个扇区。文件这样成为碎片后，每次打开该文件时计算机都必须搜索文件的所有部分，而这会增加响应时间。在 Active Directory 中，碎片整理重新安排如何将数据写入目录数据库文件以压缩之。另请参见“碎片”。

delegation / 委派

将管理名称空间空间一部分的责任指派给另一个用户、组、或者组织的能力。对 DNS 而言，是指记录于父区域中的一个名称服务，它列出被委派的区域的名称服务器权威。另请参见“继承”“繁殖”。

delegation wizard / 委派向导

用于将精确的管理员工作量的元素分配到他物的一个向导。

demand-dial connection / 请求拨号型连接

一种当需要传递数据时启动的连接，通常是用一条电路交换的广域网链接。通常，当没有业务流的时候请求拨号型连接会被终止。

demand-dial interface / 请求拨号接口

一个逻辑接口，代表一条配置于呼叫方路由器的请求拨号型连接（PPP 链路）。请求拨号接口包含诸如以下的配置信息：

要使用的端口、用来创建连接的寻址信息（例如电话号码）、身份验证与加密方法、以及身份验证凭据。

dependency / 依存关系

一个资源必须联机第二个资源才能联机的那种状态。

dependency tree / 依存关系树

通过依存关系连接到一起的资源的一个离散集。给定依存关系树中的所有资源都必须是一个单个组的成员。另请参见“依存关系”、“资源”。

desktop / 桌面

窗口、图标、菜单、以及对话框在其中显示的屏幕工作区域。

device / 设备

可以联系到一个网络或计算机的一个设备，例如一台计算机、打印机、一根操纵杆、一块适配器或调制解调器、或者任何其他外设。设备通常需要设备驱动程序来和 Windows 2000 作用。另请参见“设备驱动程序”。

device driver / 设备驱动程序

允许某特定设备（例如调制解调器、网络适配器、或打印机）和 Windows 2000 通信的程序。虽然设备可以装到系统中，但在安装并配置适当的驱动程序之前 Windows 2000 是不能使用此设备的。如果某设备列于硬件兼容列表 (HCL) 中，则通常 Windows 2000 中有其一个驱动程序。设备驱动程序在计算机启动时装载（对所有启用的设备均如此），然后就在后台运行而不为人所见。另请参见“硬件兼容列表 (HCL)”。

Dfs root / Dfs 根目录

在 Dfs 拓扑结构顶端共享的一个服务器消息块，它是组成 Dfs 名称空间的链接及共享文件的起始点。Dfs 根目录可以在域一级定义，用于基于域的操作；或者在服务器级别定义，用于独立操作。基于域的 Dfs 在域中可以有多个根，但在每个服务器上只能有一个根。

Dfs topology / 拓扑结构

一个分布式文件系统的总体逻辑层次结构，包括诸如以下的元素：根、链接、共享文件夹、复制集，正如 Dfs 管理控制台中所描述的那样。不可将其与 Dfs 名称空间混淆，后者是用户所看到的共享资源逻辑视图。

DHCP

参见“动态主机配置协议”。

DHCP Manager / DHCP 管理器

用于管理 DHCP 服务器的主要工具。DHCP 管理器是安装 DHCP 服务时添加到管理工具菜单的一个 Microsoft 管理控制台 (MMC) 工具。

DHCP Service / DHCP 服务

一个服务，它使得计算机行使 DHCP 服务器的工作并配置网络中启用了 DHCP 的客户机。DHCP 运行于一台服务器计算机，使得对 IP 地址的管理和对一个网络的客户机的其他 TCP/IP 配置的设置以集中方式自动进行成为可能。

dialog box / 对话框

一个被显示来请求或提供信息的窗口。许多对话框有一些必须被选择后 Windows NT 才能执行某一命令的选项。

digital certificate / 数字证书

参见“证书”。

directory / 目录

包含关于人们、计算机文件、或其他对象的信息的信息源（比如一个电话目录）。在文件系统中，目录保存关于文件的信息。在分布式计算环境（如 Windows 2000 域）中，目录保存诸如打印机、应用程序、数据库、以及其他用户等的信息。

directory partition / 目录分区

Active Directory 的一个连续子树，作为一个单位被复制到包含同样子树的副本的目录林中的其他域控制器。Active Directory 中，对一个域，一个服务器通常有至少三个目录分区：即构架、该目录的类别及属性定义、配置、复制拓扑结构以及相关元数据、域、包含各域对象的子树。构架和配置目录分区被复制到给定目录林中的每个域控制器。域目录分区只被复制到该域的域控制器。除了一个其自己的域目录分区的完全的、可写的副本外，一个全局编录服务器还有该目录林中所有其他的域目录分区的一个部分的、只读的副本。另请参见“完全副本”、“全局编录”、“部分副本”。

directory service / 目录服务

目录信息源及使其可得以使用的服务。目录服务使得用户给出对象的任一个属性即可查找该对象。另请参见 Active Directory、“目录”。

directory store / 目录存储区

在给定域控制器上的 Active Directory 目录分区副本的物理存储区。该存储区是用 Extensible Storage Engine（可扩展存储引擎）来实现的。

directory tree / 目录树

一个目录中的对象及容器的层次结构，可以以根对象在顶端的倒置树的图形方式看到。通常，目录树的终结点是单一（叶）对象，树中的节点或分支则为容器对象。目录树用从一个对象到另一对象的路径的方面显示了对象是如何连接起来的。。一个简单树是一个单个容器及其对象。一个连续子树是树中的任意不间断路径，包括该路径上任何容器的所有成员。

disable / 禁用

使一个设备不工作。例如，如果一个硬件配置文件中的设备已被禁用，则使用该硬件配置文件时该就不能使用该设备。禁用设备会释放分配给该设备的资源。

discovery / 发现

一个 Windows 2000 Net Logon 服务用以定位受信域中一个运行 Windows 2000 Server 的域控制器的进程。一旦发现了域控制器则将其用于后继的用户帐户身份验证。对 SNMP 而言，动态发现即为对配属于一 SNMP 网络的设备的标识。

discretionary access control list (DACL) / 任意访问控制表

一个对象的安全描述符中授权或禁止特定用户或组访问该对象的那个部分。只有对象的所有者可以更改 DACL 中授予或禁止的权限；因此对对象的访问是由其所有者任意处置的。另请参见“访问控制项”、“对象”、“ 系统访问控制列表”、“安全描述符”。

disk / 磁盘

附属于计算机的一个物理数据存储设备。另请参见“基本磁盘”、“动态磁盘”。

disk quota / 磁盘配额

一个用户可用的磁盘空间的最大值。

display adapter / 显示适配器

一个插到个人计算机中给予其显示能力的扩展电路板。计算机的显示能力即取决于逻辑电路（视频适配器中）又取决于监视器。每块适配器提供几种不同视频模式。视频模式的两个基本类别是文字的和图形的。在文字和图形模式中，一些监视器还提供对分辨率的选择。在较低分辨率下，监视器可以显示更多颜色。现代的适配器有内存，因此计算机的 RAM 不用于存储显示。另外，大多数适配器有其自己的用于图形计算的图形协处理器。这些适配器通常称为图形加速器。另请参见“网络适配器”。

distributed component object model (DCOM) / 分布式组件对象模型

定义组件如何在基于 Windows 的网络上通信的 Microsoft 组件对象模型 (COM) 规范。使用 DCOM 配置工具集成跨计算机的客户/服务器应用程序。DCOM 也可以用于集成鲁棒 Web 浏览器应用程序。另请参见“DCOM 配置工具”。

distributed DHCP / 分布式 DHCP

一种 IP 地址跨越站点边界分布的 DHCP 方案。

Distributed file system (Dfs) / 分布式文件系统

一个由存在于网络服务器和客户机上的软件组成的 Windows 2000 服务，它将位于不同文件服务器上的共享文件夹透明地连接到一单个的名称空间中以改善负载共享和数据可用性。

distribution folder / 分发文件夹

创建于 Windows 2000 分发服务器上用来包含 Setup 文件的文件夹。

distribution point / 分发点

在 System Management Server（系统管理服务器）中，承担分发点角色、存储来自站点服务器的包文件的站点系统。在检测到一个公布的应用程序可以从一个客户访问点得到后，系统 Systems Management Server（系统管理服务器）客户联系分发点以获得程序或文件。

distribution point group / 分发点组

Systems Management Server（系统管理服务器）中可以作为一单个实体来管理的一组分发点。

DNS server / DNS 服务器

一个运行 DNS 服务器程序、包含名称到 IP 地址映射、IP 地址到名称映射、有关域树结构的信息以及其他信息的计算机。DNS 服务器也试图解析客户查询。

DNS suffix / DNS 后缀

对 DNS 而言，指一个可以附加到用于名称查询或主机查找的相对域名的末尾的可选的父域名称。当查询一个名称的第一次尝试失败后，DNS 后缀可以来完成一个完全合格的替换域名称。

domain / 域

对 Windows NT 或 Windows 2000 而言，指共享 Security Accounts Manager (SAM)（安全帐户管理器）数据库并可以作为一个组来管理的一组运行 Windows NT 或 Windows 2000 的联网计算机。一个拥有某特定域的帐户的用户可以从该域中的任一计算机登录并访问其帐户。域是 Windows NT 计算机网络的一个单个安全边界。对 DNS 而言，指 DNS 树中一个节点下的一个分支。

domain consolidation / 合并域

将两个或两个以上的域合并为一个较大的域的过程。

domain controller / 域控制器

对一个 Windows NT 或 Windows 2000 域而言，指对域登录进行身份验证并维护域的安全策略及主控数据库的服务器。服务器和域控制器都能够验证用户登录，但密码只能通过与域控制器联系才能更改。

domain controller locator (Locator) / 域控制器定位器

运行于 Netlogon 服务上下文中并在 Windows 2000 网络上查找域控制器的一种算法。Locator 可以用 DNS 名称（用于和 IP/DNS 兼容的计算机）或 NetBios 名称（用于运行 Windows 3.*x*、Windows for Workgroups、Windows NT 3.5 或以后的版本、Windows 95、或 Windows 98 的计算机，或者用于不支持 IP 传输的网络中）来查找域控制器。

domain local group / 本地域组

只在本机模式域中可用并可以包含来自一个域林中的、受信林中的、或一个受信的预发行版 Windows 2000 域中的任何地方的成员的一个 Windows 2000 组。本地域组只能授予对它们所在的域中的资源的权限。通常，本地域组用于从域林收集安全负责者来控制对域内资源的访问。

domain migration / 域迁移

将帐户、资源、及其相关安全对象从一个域结构转移到另一个域结构的过程。

domain name / 域名

Windows 2000 及 Active Directory 中，是指由管理员给予的一组共享一个公有目录的联网计算机的名称。对 DNS 而言，域名是 DNS 名称空间树中的特定节点名称。DNS 域名使用由句点 (.)连接起来的叫着“标签”的单节点名称，这些单节点名称表示名称空间中的各个节点级别。另请参见“域名系统 (DNS)”、“名称空间”。

domain name label / 域名标签

完全 DNS 域名的各部分，代表域名空间目录树中的一个节点。域名由标签序列组成，例如组成 DNS 域名“noam.reskit.com” 的三个标签（”noam”、”reskit”、”com”）。DNS 名中的每个标签必须有 63 或更少的字符。

Domain Name System (DNS) / 域名系统

用于定位 Internet 或专用 TCP/IP 网络上的域名的一个层次化的名称系统。DNS 提供了一种将 DNS 域名映射到 IP 地址或进行反方向映射的服务。这允许用户、计算机、以及应用程序查询 DNS 从而用完全合格域名指定远程系统，而不是用 IP 地址指定。另请参见“ 域 ”、ping。

domain namespace / 域名空间

域名系统（DNS）所使用的数据库结构。另请参见“ 域名系统 (DNS) ”。

domain restructure / 域重构

将一个域结构重新组织成为另一个的过程，该过程通常会导致对帐户、组、以及信任的改变。

domain tree / 域树

在 DNS 中指用来索引域名的倒置的层次化树结构。在目的和概念上，域树同用于磁盘存储的计算机文件系统所用的目录树相似。另请参见“ 域名 ”、“ 名称空间 ”。

domain upgrade / 域升级

用新版本替换域中的计算机上的旧操作系统版本的过程。

domain-based Dfs / 基于域的 Dfs

一种将其配置信息保存在 Active Directory 中的 Dfs 的实现。因为该信息对域中所有的域控制器都可用，基于域的 Dfs 为

该域中任何分布式文件系统提供了高可用性。一个基于域的 Dfs 根有以下特点：它必须以一个域成员服务器为主机，它的拓扑结构被自动发布到 Active Directory，它可以有根一级的共享文件夹，而且它支持通过 FRS 的文件复制。

drain

对网络负载平衡而言，是指一个禁止端口范围包含指定端口的规则对新业务流进行处理的程序。所有在端口规则中指定的端口都会受到影响。如果对端口指定 “all”，则该命令施加于所有端口规则所覆盖的端口。对指定主机的新连接是不允许的，但是所有的活动连接还会维持下去。要禁用活动连接，请使用禁用命令。如果指定的主机没有启动群集操作，则该命令就不发生作用。另请参见 drainstop、“ 端口规则 ”。

drainstop

对网络负载平衡，指一种禁用指定的主机上对新业务流的处理的工具。禁用后主机进入 draining 模式完成现存连接。drain 时，主机保持在群集中并在再没有活动连接后停止群集操作。要终止 draining 模式，您可以通过用停止命令显式地停止群集模式或通过用开始命令重新开始处理新业务流。要从一个端口 drain 连接，请用 drain 命令。另请参见 drain。

dump file / 转储文件

以防失败发生用来在内存中保存数据的文件。

Dvorak keyboard / Dvorak 键盘

一种替换键盘，其键盘布局使得常用的字符对使用标准 QWERTY 键盘布局有困难的人更易敲击到。

dynamic disk / 动态磁盘

一种由磁盘管理所管理的物理磁盘。动态磁盘只能包含动态卷（即用磁盘管理创建的卷）。动态磁盘不能包含分区或逻辑驱动器，也不能为 MS-DOS 所访问。另请参见“动态卷”、“分区”。

Dynamic Host Configuration Protocol (DHCP) / 动态主机配置协议

一个网络协议，为计算机提供了安全、可靠、而简单的 TCP/IP 网络配置和对网际协议 (IP) 地址的动态配置。DHCP 通过对地址分配进行集中管理以确保不会发生地址冲突并协助节省 IP 地址的使用。

dynamic routing / 动态路由

使用路由协议更新路由表。动态路由对 internet 网络拓扑结构的更改会作出反应。

dynamic update / 动态更新

一个域名系统 (DNS) 的升级标准，它允许保存 DNS 中名称信息的主机动态地注册和更新其在由可以接受并处理动态更新消息的 DNS 服务器所维护的区域中的记录。

dynamic volume / 动态卷

一种用磁盘管理创建的逻辑卷。动态卷包括简单卷、跨区卷、带区卷、镜象卷和 RAID-5 卷。动态卷必须创建在动态磁盘上。另请参见“动态磁盘”、“卷”。

dynamic-link library (DLL) / 动态链接库

Microsoft Windows 系列操作系统和 OS/2 操作系统的一种功能。DLL 允许可执行例程以扩展名 .dll 单独保存，并且只在调用它的程序需要它的时候才被装入。这些例程通常为一个或一组函数服务。

E

embedded object / 内嵌对象

在另一个应用程序中创建并被粘贴到文档中的信息。信息被嵌入后，您可以用来自原程序的工具栏和菜单在新文挡中编辑它。双击嵌入的图标，则出现用来创建该对象的程序的工具栏和菜单。嵌入信息不和原文件连接在一起。如果您在某个地方更改信息，在另一个地方并不会更新。另请参见“链接对象”。

emergency repair disk (ERD) / 紧急修复磁盘

一张由备份工具所创建的磁盘，它包含关于当前 Windows 系统设置的信息。如果您的计算机不能启动，或者您的系统文件被损坏或删除了，可以用这张磁盘来修复您的计算机

emulated local area network (ELAN) / 仿真局域网络

使用局域网仿真所定义的机制来建立的逻辑网络。这可以包含 ATM 和以前配属的终端机器。

enable / 启用

使一个设备工作。例如，如果您的硬件配置设置里的一个设备已启用，则当您使用该硬件配置时这个设备就可用。

encrypted password / 加密的密码

被扰码的密码。加密的密码比明文密码更为安全，明文密码在网络窥探者面前更为脆弱。

encryption / 加密

以一种隐藏其实质的方式伪装消息或数据的过程。

encryption key / 加密密钥

由一个算法用来对消息编码或解码的值。

end-to-end encryption / 端到端加密

在客户应用程序和作为该客户应用程序所访问的资源或服务的主机的服务器之间的数据加密。

enterprise certification authority / 企业证书颁发机构

与 Active Directory 完全集成在一起的 Windows 2000 证书颁发机构。另请参见“证书颁发机构”和“独立证书颁发机构”。

entry / 项目

项目是注册表中最低级的元素。它们出现在注册表编辑器窗口的右窗格中。每个项目都由一个项目名称、其数据类型及其值组成。

它们保存影响操作系统及运行于此操作系统的程序的实际配置信息。这样，它们与键和子键不同，键和子键是容器。

项目用其注册表路径和名称来引用。一个项目中能保存的数据的量和类型由该项目的数据类型决定。

environment variable / 环境变量

由环境信息（例如驱动器、路径和文件名）组成的字符串，Windows NT 和 Windows 2000 可以通过与之相关的符号名使用它们。用户可以通过控制面板中的“系统”选项，或命令提示符下的 set 命令定义环境变量。

error detection / 错误检测

一种检测在传输过程中的数据丢失的技术。它使软件可以通过向发送计算机请求重发数据，来恢复丢失的数据。

event / 事件

指发生于系统或应用程序中，需要通知用户或向日志中添加项目的任何重要事情。

Event Log / 事件日志

记录事件日志项目的文件。

event logging / 事件记录

Windows 2000 的一个进程，每当某事件（例如服务启动和停止、用户登录和注销以及访问资源）发生时，它将记录审核轨迹中的审核项目。您可以用事件查看器审阅 Macintosh 服务事件和 Windows 2000 事件。

event types / 事件类型

错误、带时间戳的基本操作、或设备问题。

everyone category / everyone 的分类

Macintosh 环境中的一种用户类别，该类别被指派了文件夹的权限。权限授予 everyone 后，将适用于包括来宾在内的所有使用该服务器的用户。

expire interval / 过期间隔

对 DNS 而言，指 DNS 服务器作为一个区域的辅助服务器运作的秒数，当区域没有被刷新或更新时用来决定区域数据是否过期。另请参见“ 区域 ”。

explicit trust relationship / 显式信任关系

来自 Windows NT 的信任关系，在此关系中只能在一个方向上建立显式链接。显式信任也可以存在于 Windows NT 域和 Windows 2000 域之间，或森林之间。

export / 导出

NFS 中，服务器使文件系统可以被客户装载。

extended partition / 扩展分区

基本磁盘的一部分，它可以包含逻辑驱动器。要想在基本磁盘上有多于四个的卷，则需要使用扩展分区。每个物理磁盘只允许四个分区中的一个是扩展分区，并且创建扩展分区不需要有主分区存在。只能在基本磁盘上创建扩展分区。另请参见“ 基本磁盘 ”、“ 逻辑驱动器 ”、“ 分区 ”、“ 主分区 ”、“ 未分配空间 ”。

Extensible Authentication Protocol (EAP) / 可扩展的身份验证协议

PPP 的一个扩展，允许对 PPP 连接的验证采用任意的身份验证机制。

external network number / 外部网络号

一个用于寻址和路由目的的 4 字节十六进制号码。外部网络号与物理网络适配器和网络相关联。为了相互通信，同一网络中使用给定帧类型的所有计算机都必须具有同样的外部网络号。对 IPX 互连网络而言，所有外部网络号必须是唯一的。另请参见“ 内部网络号 ”、“ 网际数据包交换 (IPX) ”。

external routes / 外部路由

一条不在 OSPF 自治系统中的路由。

extranet

公用网络（典型为 Internet）中计算机或用户的有限子集，它由能够访问组织内部网络的计算机或用户组成。典型地，这些计算机或用户属于合作组织。

eye-gaze pointing device / 目控定点设备

一种通过视觉控制屏幕光标的输入设备，它允许用户按下对话框中的屏幕按钮、选择菜单项和选择单元格或文本。

F

failback (v., fail back) / 故障回复

在服务器群集中，将一个发生故障的组移动到该组“ 首选所有者 ”列表的下一节点。另请参见“ 故障转移 ”、“ 节点 ”、“ 资源 ”。

failover (v., fail over) / 故障转移

在服务器群集中，一种提高可用性的方法。一旦组的资源或者组联机的节点发生故障时，群集会让该节点上的组脱机，然后把该组联机到其它节点。请参见“ 节点 ”、“ 资源 ”。

FAT32

这是一个文件分配表文件系统的派生系统。FAT32 与 FAT 相比支持更小的簇，因此，在 FAT32 驱动器上的空间分配效率更高。另请参见“ 文件分配表 (FAT) ”、“ NTFS 文件系统 ”。

fault tolerance / 容错

硬件发生故障时保证数据完整性的一种功能。在 Windows NT 和 Windows 2000 操作平台上，容错功能是由 Ftdisk.sys 驱动程序提供的。

FDDI

请参见“ 光纤分布式数据接口 ”。

Fiber Distributed Data Interface (FDDI) / 光纤分布式数据接口 (FDDI)

一种设计用于光纤电缆布线的网络媒体。另请参见“ LocalTalk ”、“ 令牌环 ”。

file allocation table (FAT) / 文件分配表 (FAT)

一个基于文件分配表 (FAT) 的文件系统。一些操作系统包括 Windows NT 和 Windows 2000 仍保留它，用来跟踪文件存储磁盘空间各区段的状态。

File Replication service / 文件复制服务

分布式文件系统（Dfs) 用来同步指定复制内容的一种服务，同时 Active Directory 站点和服务用它在域控制器间复制拓扑和全局编录信息。

file server / 文件服务器

在一个组织范围内提供文件、程序和应用程序访问的服务器。

file system / 文件系统

操作系统中文件命名、存储和组织的总体结构。NTFS、FAT 和 FAT32 是不同类型的文件系统。

File Transfer Protocol (FTP) / 文件传送协议 (FTP)

一项定义如何在 Internet 上和客户/服务器应用程序（这些应用程序使用该协议传送文件）中将文件从一台计算机传送到其它计算机的协议。

filter / 筛选器

IPSec 中，为基于源、目标和 IP 通信类型的通讯提供触发安全协商功能的规则。

filtering mode / 筛选模式

对于网络负载平衡，是指群集内主机处理流入该群集的网络通信的方法。通信可以由单一服务器处理，也可以在群集内的主机间平衡负载，或者完全禁用。另请参见“ 服务器 ”。

FilterKeys / 筛选键

Windows 2000 的一个辅助功能，它允许身体残疾者调整键盘的响应时间。另请参见“ 回弹键 ”、“ 重复键 ”、“ 慢键 ”。

filters / 筛选器

IP 和 IPX 数据包筛选中，一系列向路由器说明每个接口所允许和禁止的通信类型的定义。

firewall / 防火墙

一个提供安全系统的硬件和软件组合，一般是为了防止外部对内部网或 Intranet 的未经授权的访问。防火墙可以路由通过网络外部代理服务器的通讯，从而阻止网络和外部计算机间的直接通讯。代理服务器确定让文件传到网络上是否安全。防火墙又被称为“ 具有安全利刃的网关 ”。

folder redirection / 文件夹重定向

一个允许您将指定文件夹重定向到网络的组策略选项。

forest / 目录林

一个或多个 Windows 2000 Active Directory 目录树的集合，这些目录树被对等地组织起来，并通过每个目录树的根域间的双向可传递信任关系连接起来。一个目录林中的所有目录树共享一个公用的构架、配置和全局编录。当一个目录林包含多个目录树时，这些目录树不会形成毗邻的名称空间。

form / 格式

用来指定分配给打印机送纸器的纸张大小（比如 letter 或 legal）。格式定义了诸如纸张大小以及纸张或其它打印媒体的打印机区域边距等物理参数。

FORTEZZA

一系列安全产品，包括 PCMCIA 卡、兼容串行端口设备、组合卡（比如 FORTEZZA/Modem 和 FORTEZZA/Ethernet）、服务器板等等。FORTEZZA 是 National Security Agency 的注册商标。

fractional T1 / 部分 T1 连接

由 23 个 B 信道和一个 D 信道组成的 T1 线路。这个单一的 D 信道用于计时。

fragmentation / 碎片

同一个磁盘文件被分散到磁盘不同区域的各个部分。在磁盘上删除文件或添加新文件时，都会产生碎片。碎片会降低磁盘的访问速度，降低磁盘操作的整体性能，尽管一般来说并不严重。另请参见“ 碎片整理 ”。

frame / 帧

在异步通讯中，从一个设备传送到其他设备的信息包，是信息传送的单位。帧这个术语最常用于以太网中。帧类似于其它网络中用到的数据包。另请参见“ 数据包 ”。

free space / 可用空间

扩展分区中可用于创建逻辑驱动器的空间。另请参见“ 扩展分区 ”、“ 逻辑驱动器 ”、“ 未分配空间 ”。

FTP

请参见“ 文件传送协议 ”。

full replica / 完全复制

一种目录分区的读/写复制，它包含了这个分区中所有对象的所有属性。完全复制又称为主复制。另请参见“ 部分复制 ”。

full zone transfer (AXFR) / 完全区域复制 (AXFR)

所有 DNS 服务器都支持的标准查询类型，用来在区域更改时更新和同步区域数据。当使用 AXFR 作为指定查询类型进行 DNS 查询时，作为响应，整个区域都被复制。另请参见“ 增量区域复制 (IXFR) ”、“ 区域 ”、“ 区域复制 ”。

fully qualified domain name (FQDN) / 完全合格的域名称 (FQDN)

一个规定的 DNS 域名，用以说明它在域名空间目录树中的准确位置。例如 client1.reskit.com。FQDN 又称为“ 完整的计算机名称 ”。

G

gateway / 网关

一种连接到多个物理 TCP/IP 网络的设备，能够在网络间路由或发送 IP 数据包。网关能够完成不同传输协议和数据格式（例如 IPX 和 IP ）间的转换，通常把网关加到网络中正是由于它具有这种转换功能。另请参见“ IP 地址 ”、“ Internet 协议路由器 ”。

Gateway Service for NetWare / NetWare 网关服务

一项创建一个网关让 Microsoft 客户能够通过 Windows 2000 服务器访问 NetWare 核心协议网络的服务，如 NetWare 文件和打印服务。

generic Quality of Service / 一般服务质量

TCP/IP 网络为多媒体应用程序提供的一种服务质量保证方法。“ 一般服务质量 ”为每个连接按需分配不同的带宽。

Gigabit Ethernet / 千兆位以太网

以每秒 10 亿位或更高速率传输数据的以太网标准。

Global Catalog / 全局编录

一种将来自所有源域的目录信息存储到安装目录树下单一位置的 Active Directory 服务。用户可以向全局编录提交有关对象的查询，

而无须考虑该对象的逻辑和物理位置。全局编录为解决查询作了性能优化。

global group / 全局组

对 Windows 2000 Server 来说，是指可以用在自身的域中、域的成员服务器和工作站中，以及信任域中的组。在所有位置，全局组都可以被赋予权利和权限，成为本地组的成员。但全局组只能包含自身域中的用户帐户。另请参见“组”、“本地组”。

globally unique identifier (GUID) / 全局唯一标识符 (GUID)

一个由设备唯一标识符、当前日期和时间、以及一个顺序号生成的 16 字节值。GUID 用来标识一个特定的设备或组件。

graphical user interface (GUI) / 图形用户界面 (GUI)

象 Windows 那样，使用图形映像（如按钮和图标）来表示程序功能的一种显示格式。GUI 允许用户通过指向并单击鼠标就能执行操作和做出选择。

group / 组

组是用户、计算机、联系人和其它组的集合。组可以用作安全措施，或者作为 e-mail 分布集合。分布组只用于 e-mail。安全组可用于授权对资源的访问，也可以用于 e-mail 分布列表。在服务器群集中，组是资源的集合，是故障转移的基本单位。另请参见“本地域组”、“全局组”、“本机模式”、“通用组”。

group memberships / 组成员身份

用户帐户所属的那些组。赋予组的权限和权利，也同时赋予组的成员。在大多情况下，用户在 Windows 2000 中可以执行的操作取决于用户登录的用户帐户的组成员身份。另请参见“组”。

Group Policy / 组策略

一个管理员工具，用于定义和控制程序、网络资源和操作系统为一个单位中的用户和计算机执行操作的方式。在 Active Directory 环境中，“组策略”根据用户和计算机在站点、域或部门中的成员身份，应用到他们身上。

Group Policy object / 组策略对象

一个组策略设置的集合。组策略对象是由组策略管理单元创建的文档。组策略对象在域层次上存储，并影响站点、域和部门中的用户和计算机。每个基于 Windows 2000 的计算机都在本地存储了一组设置，称为“本地组策略对象”。

guest / 来宾

为没有用户帐户或没有密码的 Macintosh 用户提供的一项服务。如果 Macintosh 用户将权限分配给每个人，这些权限也会给予来宾和这个组的用户。

guest account / 来宾帐户

用户没有该计算机、该域或者任何该计算机域信任的域的帐户时，用来登录到 Windows 2000 计算机的一个内建帐户。

GUI mode / GUI 模式

安装程序中使用图形用户界面 (GUI) 的部分。

H

handle / 句柄

用户界面中，是指添加到对象上的接口，以方便移动对象、改变对象大小、调整对象形状及其它与对象相关的操作。在编程时是指指向指针的指针 — 也就是能让程序访问指定资源的一个标记。

hardware abstraction layer (HAL) / 硬件抽象层 (HAL)

硬件制造商提供的一薄层软件，它将硬件的差异从操作系统的更高层中隐藏或抽象出来。通过 HAL 提供的筛选器，不同类型的硬件在操作系统的其余部分看来都是相同的。这允许 Windows NT 和 Windows 2000 从一种硬件平台移植到其它硬件平台。HAL 还提供了一些例程，允许单个设备驱动程序支持同一设备在所有平台上正常工作。HAL 和内核一起紧密运行。

hardware compatibility list (HCL) / 硬件兼容列表 (HCL)

Windows 2000 所支持的设备列表。

hardware failure / 硬件故障

一个物理组件的故障，比如磁盘头故障或内存错误。

hardware inventory / 硬件清单

Systems Management Server 用来收集 Systems Management Server 站点内客户计算机所用硬件详细信息的自动程序。

hardware router / 硬件路由器

专门执行路由的路由器，其硬件经特殊设计并为路由作了优化。

hardware type / 硬件类型

相似设备的一个分类。例如，图像处理设备是数字照相机和扫描仪的硬件类型。

heartbeat / 心跳

在服务器群集或网络负载平衡群集中，在节点间发送的周期性消息，以检测节点的系统故障。

hexadecimal / 十六进制

基于 16 进制的系统，其数值用从 0 到 9 的数字以及从 A （等于十进制的 10）到 F （等于十进制的 15 ）的字母来表示。

hierarchical storage management (HSM) / 分级存储管理 (HSM)

一种通过自动将不常访问的文件从本地存储迁移到远程存储，并根据用户要求撤回文件，而使存储管理自动化并降低存储成本的技术。

high availability / 高可用性

保证应用程序或服务在大多数时间运行并可供客户使用的能力。

hop count / 跃点计数

表示处理 IPX 数据包的 IPX 路由器数量的传输控制域。

host / 主机

运行服务器程序，或者网络或远程客户使用的服务的 Windows 2000 计算机。为了网络负载平衡，一个群集包含多个连接在局域网上的主机。

host ID / 主机 ID

用来标识由路由器界定的物理网络接口的数字。主机 ID 在网络中应该是唯一的。

host name / 主机名

网络上计算机的名称。在 Windows 2000 Server Resource Kit 中，主机名用来指完全合格域名的第一个标签。另请参见“主机文件”。

host priority / 主机优先级

对“网络负载平衡”，是指主机处理 TCP 和 UDP 端口默认网络通信的优先权。它在群集中的主机脱机时用到，用来确定群集中的哪一台主机负责处理以前由脱机的主机处理的通信。另请参见“用户数据报协议 (UDP)”。

Hosts

一个包含已知 IP 地址列表的文件，TCP/IP 用它来定位网络或 Internet 上的计算机。

hosts file / 主机文件

一个与 4.3 Berkeley Software Distribution (BSD) UNIX/etc/hosts file 格式相同的本地文本文件。

这个文件将主机名映射成 IP 地址。Windows 2000 中，该文件存放在 \%Systemroot%\System32\Drivers\Etc 文件夹。另请参见 systemroot。

hot keys / 热键

Windows 2000 的一个功能，它允许同时按下组合键将指定的辅助功能迅速激活。

hub / **网络集线器**

将通讯线路连接到一个中心位置的网络设备，它向网络上的所有设备提供公用的连接。

Hub-and-Spoke / 网络集线器与辐条

一个 WINS 服务器配置，用一个中心“网络集线器”作为联系很多无关 WINS 服务器“辐条”的点，以改善集中时间。

Hypertext Markup Language (HTML) / 超文本标记语言 (HTML)

一种简单的标记语言，用来创建可在平台间移动的超文本文档。HTML 文件是一些简单的 ASCII 文本文件，包含了内嵌编码（用一些标记表示）来表示格式编排和超文本链接信息。HTML 用于万维网上的文档格式编排。

Hypertext Transfer Protocol (HTTP) / 超文本传输协议 (HTTP)

用来在万维网上传输信息的协议。HTTP 地址（一种 URL 或“统一资源地址”）采用如下格式：
http://www.microsoft.com

I

IKE

请参见“ Internet 密钥交换 ”。

impersonation / 模拟

Windows 2000 Server 允许一个进程采用另一个进程的安全属性时发生的情形。

Impersonation token / 模拟令牌

一个为了捕获客户进程的安全信息而创建的访问令牌，它允许服务“ 模拟 ”安全操作中的客户进程。另请参见“ 访问令牌 ”、“ 主令牌 ”。

incremental zone transfer (IXFR) / 增量区域复制 (IXFR)

一种备用查询类型，在一个区域更改时，一些 DNS 服务器可以用它来更新和同步区域数据。如果 DNS 服务器间支持增量区域复制，服务器可以只跟踪和传输在区域的各版本间增加的资源记录更改。另请参见“ 完全区域复制 (AXFR) ”、“ 区域 ”、“ 区域复制 ”。

infrared (IR) / 红外线 (IR)

色谱中红光之外的光。这种光在人眼可视范围之外，而红外发送和接收设备能发送和接收红外信号。另请参见“ 红外数据协会 ”、“ 红外设备 ”、“ 红外端口 ”。

Infrared Data Association (IrDA) / 红外数据协会 (IrDA)

一项用来传输红外设备产生的数据的网络协议。红外数据协会同时也是建立计算机和外围设备如打印机间红外通讯标准的，计算机、组件和电讯供应商的行业组织名称。另请参见“ 红外 ”、“ 红外设备 ”、“ 红外端口 ”。

infrared device / 红外设备

能够用红外线通讯的计算机，或者是计算机的外围设备，比如打印机。另请参见“ 红外线 ”。

infrared port / 红外端口

在计算机上使用红外线（不需要电缆）与其它计算机或设备进行通讯的光学端口。红外端口可以在一些便携式计算机、打印机和照相机上看到。红外端口也可以通过将一 IR 硬件锁（即

硬件密钥安全设备）连接到 PCI 卡、串行端口、并口（用于打印机）或者直接连接到主板的方式添加到计算机上。另请参见“ 红外设备 ”、“ 红外端口 ”。

inheritance / 继承

从已有的对象类别创建新的对象类别的功能。新对象定义为原对象的一个子类别。而原对象成为新对象的超类别。子类别继承了超类别的属性，包括结构规则和内容规则。

insertion point / 插入点

打字时文字将被插入的位置。插入点在应用程序窗口或对话框中通常以闪烁的垂直条的形式出现。

install / 安装

当指软件时，是指将程序文件和文件夹添加到硬盘，并把相关数据添加到注册表，以使软件能正常运行。“ 安装 ”和“ 升级 ”不同，升级是指现存的程序文件、文件夹和注册表项目更新为更新的版本。当指硬件时，是将设备连接到计算机，加载设备驱动程序，并配置设备属性和设置。另请参见“ 设备驱动程序 ”、“ 注册表 ”。

integrity / 完整性

一种 Internet 协议安全属性，用来保护数据、避免在传送过程中发生未经授权的更改，保证接收到的数据和发送的数据完全相同的。哈希功能使用加密校验和在每个数据包上签名，接收的计算机会在打开数据包之前检查这个校验和。如果这个数据包 — 也包括签名 — 更改过，数据包会被放弃。

IntelliMirror

一组用于更改桌面和配置管理的 Windows 2000 功能。当在服务器和客户两端都使用 IntelliMirror 时，用户的数据、应用程序以及设置都会在他们移到另一台计算机时带过去。管理员可以用 IntelliMirror 完成 Windows 2000 的远程安装。

interface / 接口

在网络中，是指发送和接收数据包的逻辑设备。在路由和远程访问管理工具中，是指可以通过 LAN 或 WAN 适配器接通的网段的可视描述。每个接口都有一个唯一名称。另请参见“ 局域网 (LAN) ”、“ 网络适配器 ”、“ 路由 ”、“ 广域网 (WAN) ”。

internal namespace / 内部名称空间

一个只有单位内部的用户才能使用的专用名称空间。

internal network number / 内部网络号

一个用于寻址和路由的 4 字节十六进制号码。内部网络号标识了计算机内部的虚拟网络。内部网络号对 IPX 互连网络而言必须是唯一的。内部网络号也称为“ 虚拟网络号 ”。另请参见“ 外部网络号 ”、“ 网际数据包交换 (IPX) ”。

internet / 互连网

通过路由器连接的两个或更多网段。它是“ 互连网络 ”的另一个术语。使用 Macintosh 服务，可以将两个或更多 AppleTalk 网络连接到 Windows 2000 Server 的计算机上，以创建互连网。使用 TCP/IP，可以将两个或更多 IP 网络连接到一个运行 Windows 2000 Server 或 Windows 2000 Professional 的多宿主计算机上，创建互连网。为了在相连的 IP 网段间实现路由，必须启用 IP 转发。

Internet

由很多网络组成的全球公用 TCP/IP 互连网络，连接了研究机构、大学、图书馆以及私人公司。

Internet Assigned Numbers Authority (IANA) / Internet 授权号码委员会 (IANA)

委派 IP 地址并把地址分配给各个单位的机构，比如 InterNIC。

Internet Control Message Protocol (ICMP) / 网际消息控制协议 (ICMP)

TCP/IP 套件中必需的一项维护协议，能够报告错误，允许方便的连接。ping 工具使用 ICMP 来执行 TCP/IP 故障排除。

Internet Engineering Task Force (IETF) / Internet 工程任务组 (IETF)

由关心 Internet 体系结构发展和 Internet 正常运转的网络设计师、运营商、供应商和研究人员组成的一个开放团体。在这里，按照主题领域（比如路由、传输和安全）并通过邮件列表组织的工作组，来执行技术任务。Internet 标准是在 IETF Requests for Comments （注释请求，RFC ）中开发出来的，RFC 是一系列讨论计算和计算机通讯各个方面问题的注意事项，集中于网络协议、程序和概念。

Internet Group Management Protocol (IGMP) / Internet 组管理协议 (IGMP)

TCP/IP 协议组中的一项协议，负责 IP 多播组员身份的管理。

Internet Information Services (IIS) / Internet 信息服务 (IIS)

支持 Web 站点创建、配置和管理的软件服务，和其它 Internet 功能一起提供。Internet 信息服务包括网络新闻传送协议（NNTP)、文件传送协议（FTP)、以及简单邮件传送协议（SMTP)。另请参见“ 文件传送协议 (FTP) ”、“ 网络新闻传送协议 (NNTP) ”、“ 简单邮件传送协议 (SMTP) ”。

Internet Key Exchange (IKE) / Internet 密钥交换 (IKE)

一项建立安全关联和共享密钥的协议，双方使用 Internet 协议安全进行通讯时必须使用共享密钥。

Internet Protocol (IP) / Internet 协议 (IP)

TCP/IP 协议组中的一项可路由协议，负责 IP 寻址、路由、以及碎片整理和 IP 数据包的重新组装。

Internet Protocol router / Internet 协议路由器

一个连接到多个物理 TCP/IP 网络的系统，能够在网络间路由或传递 IP 数据包。另请参见“ 数据包 ”、“ 路由器 ”、“ 路由 ”、 “ TCP/IP ”。

Internet Protocol security (IPSec) / Internet 协议安全 (IPSec)

一组工业标准、基于加密的保护服务和协议。使用 L2TP，IPSec 保护 TCP/IP 协议组和 Internet 通讯中的所有协议。另请参见“ 第二层隧道协议 (L2TP) ”。

Internet service provider (ISP) / Internet 服务提供商 (ISP)

为个人和公司提供 Internet 和万维网接入服务的公司。ISP 会提供一个电话号码、用户名和密码以及其它连接信息，让用户可以将计算机连到 ISP 的计算机上。一般 ISP 按每月和/或每小时的连接费用进行收费。

internetwork / 互连网络

使用路由器连接起来的至少两个网段。

Internetwork packet exchange (IPX) / 网际数据包交换 (IPX)

NetWare 开发的网络协议，负责控制数据包在 LAN 内或 LAN 间的寻址和路由。IPX 并不保证消息的完整性（没有丢失的数据包）。另请参见“ 网际数据包交换/顺序数据包交换 (IPX/SPX) ”。

intranet

一个组织内部的网络，它使用 Internet 技术和协议，但只对特定的人才可用，比如公司的员工。Intranet 也称为“ 专用网络 ”。

inventory / 清单

Systems Management Server 清单客户代理为站点内的每个客户收集的信息。

清单可以包括硬件和软件信息以及收集的文件，这取决于管理员定义的配置。

IP address / IP 地址

一个 32 位地址，用于标识 IP 网络上的节点。必须为 IP 网络上的每个节点都分配一个唯一 IP 地址，由网络 ID 加上唯一主机 ID 构成。这个地址一般用以圆点隔开的八进制数的十进制值来表示（例如，192.168.7.27 ）。在 Windows 2000 中，IP 地址可以通过 DHCP 手动或动态配置。另请参见“ 动态主机配置协议 (DHCP) ”、“ 节点 ”。

IPSec

请参见“ Internet 协议安全 ”。

IPSec driver / IPSec 驱动程序

一种 Internet 协议安全机制，在计算机配置了 Internet 协议安全时被激活，负责监视数据包，看它们与计算机中当前 Internet 协议安全策略的 IP 筛选器是否匹配。IPSec 驱动程序同时会执行实际的数据加密和解密。另请参见“ Internet 协议安全 ”。

IPSec driver / IPSec 驱动程序

使用当前 IPSec 策略的 IP 筛选器列表的驱动程序，负责监视出站 IP 数据包的安全性以及进站信息包的验证和解密。

K

Kerberos authentication protocol / Kerberos 身份验证协议

用于验证用户或主机标识的身份验证机制。Kerberos v5 协议是 Windows 2000 默认的身份验证服务。Internet 协议安全和 QoS 许可控制服务使用 Kerberos 协议进行身份验证。另请参见“ QoS 许可控制服务 ”、“ Internet 协议安全 (IPSec) ”。

key / 密钥，键

读取、修改和验证被保护数据时所需的一个机密代码或数字。密钥与算法一起使用来保护数据。Windows 2000 会自动处理密钥的生成。对于注册表，key （键）是指一条注册表项目，可以同时包含子键和项目。在注册表结构中，键类似于文件夹，项目类似于文件。在注册表编辑器（Registry Editor）窗口中，键以文件夹形式出现在左窗格。在应答文件里，key （键）是一些字符串，指定了一些参数，在操作系统无人值守安装时安装程序从这些参数获取所需数据。

key distribution center (KDC) / 密钥分发中心 (KDC)

提供 Kerberos 身份验证协议用到的会话票据和临时会话密钥的一项网络服务。在 Windows 2000 中，KDC 作为一个优先进程在所有的域控制器上运行。KDC 使用 Active Directory 管理敏感的帐户信息，比如用户帐户的密码。另请参见“ Kerberos 身份验证协议 ”、“ 会话票据 ”。

key exchange / 密钥交换

联机密钥的保密交换，通常由公钥密码系统完成。另请参见“ 公钥密码系统 ”。

key management / 密钥管理

公钥密码系统私钥的安全管理。Windows 2000 使用 CryptoAPI 和 CSP 进行私钥的管理并为它们保密。

另请参见“私钥”、“CryptoAPI”、“加密服务提供商”。

key pair / 密钥对

一个私钥和相应的公钥。另请参见“公钥/私钥对”。

keyboard filters / 键盘筛选器

特殊的正时设备及其它设备，负责补偿异常的震动、响应时间慢及其它行动障碍。

L

L2TP

请参见“第二层隧道协议”。

label / 标签

请参见“域名标签”。

LAN

请参见“局域网络”。

LAN emulation (LANE) / LAN 仿真 (LANE)

一组允许现有的以太网和令牌环 LAN 服务覆盖 ATM 网络的协议。LANE 允许与 LAN 及 ATM 相连的机器相互连接。另请参见“异步传输模式 (ATM)”。

LAN emulation client (LEC) / LAN 仿真客户 (LEC)

仿真局域网络 (ELAN) 上执行数据转发、地址解析和其它控制功能的客户。LEC 位于仿真局域网络 (ELAN) 的终端机器上。另请参见“异步传送模式”、“仿真局域网络 (ELAN)”、“ LAN 仿真”。

LAN emulation server (LES) / LAN 仿真服务器 (LES)

仿真局域网络 (ELAN) 的中心控制点。它让 LANE 客户能够加入到仿真局域网络 (ELAN)，并将 LAN 地址解解析到 ATM 地址。另请参见 “仿真局域网络 (ELAN)”、“ LAN 仿真 (LANE)”。

LAN manager replication / LAN 管理器复制

Windows NT 下用到的文件复制服务。请参见“文件复制服务”。

large window support / 大窗口支持

TCP 通讯中，不需要确认就能传送的最大数据量。这个窗口有固定的大小。大窗口支持动态地重算窗口的尺寸，允许同一时间更大数量的数据传送，因此形成更大的吞吐量。

latency / 潜伏期

请参见“复制潜伏期”。

layer 2 tunneling protocol (L2TP) / 第二层隧道协议 (L2TP)

一项封装 PPP 帧，并通过 IP、X.25、帧中继、或 ATM 网络将其发送的隧道协议。L2TP 是点对点隧道协

议 (PPTP) 和第二层转发 (L2F) 的组合，是由 Cisco Systems, Inc. 开发的一项技术。

LDAP API

请参见“ 轻型目录访问协议访问编程接口 ”。

license service / 许可证服务

终端服务里的一台服务器存储了为终端服务下载的所有客户许可证，并跟踪已颁发给客户计算机或终端的许可证。

Lightweight Directory Access Protocol (LDAP) / 轻型目录访问协议 (LDAP)

一项直接在 TCP/IP 上运行的目录服务协议，是 Active Directory 的主要访问协议。LDAP version 3 是由 Internet 工程任务组 (IETF) RFC 2251 中一组“ 提议标准 ”文档定义的。另请参见“ 轻型目录访问协议访问编程接口 (LDAP API) ”。

Lightweight Directory Access Protocol Access Programming Interface (LDAP API) / 轻型目录访问协议访问编程接口 (LDAP API)

符合 LDAP 协议的一组底层 C 语言 API。

Line Printer Daemon (LPD) / 行式打印机守护程序 (LPD)

打印服务器上的一项服务，负责从运行于客户系统上的远程行式打印机 (LPR) 工具接收文档（打印作业）。另请参见“ 远程行式打印机 (LPR) ”。

Line Printer Remote (LPR) / 远程行式打印机 (LPR)

客户系统上运行的一个实用连接程序，用于将文件打印到运行 LPD 服务器程序的计算机。另请参见“ 行式打印机守护程序 (LPD) ”。

link state database (LSDB) / 线路状态数据库 (LSDB)

由 OSPF 路由器维护的区域的映射。在网络拓扑更改后，它会被更新。线路状态数据库用于计算 IP 路由，在网络拓扑的每次更改之后 IP 路由都必须重新计算。另请参见“ 开放最短路径优先 （OSPF） ”。

linked object / 链接对象

插入到文档，但仍存在于源文件中的对象。信息被链接时，如果源文档中的信息发生更改，则新文档会自动更新。另请参见“ 内嵌对象 ”。

load-balancing / 负载平衡

通过 Windows Clustering 将客户请求分配到群集中的多个服务器，调整基于服务器的程序（比如 Web server）的性能。各主机可以指定要处理的负载百分数，或者将负载平均分配给所有主机。如果一台主机发生故障，Windows Clustering 会动态地在剩余的主机间重新分配负载。另请参见“ 客户请求 ”、“ 群集 ”、“ 主机 ”、“ 可扩展性 ”、“ 服务器 ”。

local area network (LAN) / 局域网络 (LAN)

连接一组位于相对有限范围内（如一座建筑内）的计算机、打印机和其它设备的通讯网络。LAN 允许任一连接设备与网络上的其它设备进行交互。另请参见“ 广域网 (WAN) ”。

local computer / 本机，本地计算机

用户当前登录到的计算机。更明确一些，本机是指可以直接访问，而不需用通讯线路或者通讯设备，比如网络适配器或调制解调器访问的计算机。类似地，运行本地程序是指在您的计算机上运行程序，这与从服务器上运行程序形成对照。

local group / 本地组

对于运行 Windows 2000 Professional 的计算机和成员服务器，是指那些被从组所在的计算机上赋予了只对自己的计算机资源有权限和权利的组。另请参见“全局组”。

local printer / 本地打印机

直接连接在您的计算机端口上的打印机。

local storage / 本地存储

对于 Windows 2000 Server 时，是指用作主要数据存储的 NTFS 磁盘卷。通过将不常用文件复制到远程或辅助存储，“远程存储”可以管理这些磁盘卷。另请参见“远程存储”。

LocalTalk

置于每台 Macintosh 计算机内的 Apple 网络硬件。LocalTalk 包括电缆和连接器盒，用来连接 AppleTalk 网络系统中的组件和网络设备。LocalTalk 以前称为 AppleTalk Personal Network （ AppleTalk 个人网络）。

lock / 锁定

使一个文件无法访问。当不只一个用户可以对文件操作时，这个文件在一个用户访问时被锁定，以避免多个用户同时修改它。

log file / 日志文件

一个存储应用程序、服务或操作系统产生的消息的文件。这些消息用来跟踪已执行的操作。例如，Web server 会维护日志文件，列出到该服务器的每条请求。

日志文件通常是一些 ASCII 文件，并以 .log 作为扩展名。 备份时，是指包含磁带创建日期的记录，以及成功备份和存储的文件和目录名称的文件。性能日志和警报服务也会创建日志文件。

log off / 注销

停止使用网络，注销会将用户名从当前使用中移走，直到用户重新登录。

log on / 登录

通过提供用户名和密码标识网络用户，以开始使用网络。

logical drive / 逻辑驱动器

在基本磁盘的扩展分区里创建的卷。用户可以格式化逻辑驱动器，为其指派驱动器号。只有基本磁盘才能包含逻辑驱动器。一个逻辑驱动器不能跨越多个磁盘。另请参见“基本磁盘”、“基本卷”、“扩展分区”。

logical IP subnet (LIS) / 逻辑 IP 子网（LIS）

属于同一 IP 子网的一组 IP 主机/成员，其主机 ATMARP 服务器 ATM 地址也要相同。

logical printer / 逻辑打印机

Windows 2000 中操作系统和打印机间的软件界面。打印机是执行实际打印任务的设备，而逻辑打印机则是打印服务器上的软件界面。软件界面会确定如何处理打印作业，如何将其路由到目标（到本地或网络端口、到文件、或到远程打印共享设备）。在打印文档时，文档会在发送到打印机本身之前，先“后台打印”（或存储）到逻辑打印机上。另请参见“后台打印”。

loopback option / 环回选项

一个管理员选项，允许实施用户登录的计算机的“组策略”设置，即使已经完成了用户设置。

M

master domain / 主域

拥有用户帐户数据的 Windows NT 域。也称为“帐户域”。

master server / 主服务器

在 DNS 区域复制中，指作为区域源的计算机。主服务器可以不同，是两种类型（主主控或副主控）之一，取决于服务器获得区域数据的方式。另请参见“主服务器”、“辅助服务器”、“区域”、“区域复制”。

maximum password age / 密码最长期限

用户可以在系统要求更改密码之前使用该密码的那段时间。

media access control / 媒体访问控制

Windows NT 和 Windows 2000 网络体系结构中的一层，它处理网络访问和冲突检测。

media access control address / 媒体访问控制地址

用于在同一子网中网卡间通讯的地址。每个网卡都有相应的媒体访问控制地址。

member server / 成员服务器

运行 Windows 2000 Server 但不是 Windows 2000 域的域控制器的计算机。成员服务器参与域，但不存储目录数据库的副本。可以设置成员服务器资源的权限，以允许用户连接到服务器并使用其资源。资源权限可以赋予域全局组和用户，也可以赋予本地组和用户。另请参见“域控制器”、“全局组”、“本地组”。

metric / 指标

表示 IP 路由表中路径成本的数字。这样，可以在到达同一目标的多条路径中选择最好的路径。

Microsoft Component Services / Microsoft 组件服务

在 Internet 或其它服务器上运行的程序，负责为客户机的用户管理应用程序和数据库事务请求。组件服务让用户和客户计算机没有必要向不熟悉的数据库发出请求，并将这些请求转发到数据库服务器。它还负责管理安全、与其它服务器的连接及事务的完整性。

Microsoft Management Console (MMC) / Microsoft 管理控制台 (MMC)

一个为管理控制台提供主机服务的框架。控制台由控制台树上的项目所定义。控制台树可包括文件夹或其它容器、万维网页面及其它管理项目。一个控制台有一个或多个窗口，可提供控制台树和管理属性、服务、及控制台树项目激活的事件的视图。主 MMC 窗口提供操纵控制台的命令和工具。当控制台处在“用户模式”时，MMC 和控制台树的操纵功能可能会隐藏起来。另请参见“控制台树”。

migrate / 迁移

将文件或程序从旧文件格式或协议移动到更新的格式和协议的过程。例如，WINS 数据库项目可以从静态 WINS 数据库项目迁移到动态注册的 DHCP 项目。

migration / 迁移

将对象从本地存储区复制到远程存储区的过程。

Mini-Setup wizard / 最小安装向导

计算机从复制硬盘上启动引导程序的第一次启动的向导。该向导会收集新复制的硬盘所需的所有信息。

minimum password length / 最短密码长度

密码可以包含的最少字符数。

minimum TTL / TTL 最小值

以秒为单位设置的默认生存时间 (TTL) 值，用于区域内的所有资源记录。各区域的 TTL 最小值在起始颁发机构 (SOA) 资源记录中设置。默认情况下，DNS 服务器会在查询应答中包括该值，以通知收件人在存储的记录数据过期之前能够存储和使用查询应答中提供的资源记录多长时间。如果为单个资源记录设置了 TTL 值，则这些 TTL 值会替代 TTL 最小值。另请参见“生存时间 (TTL)”。

miniport drivers / 小型端口驱动程序

连接中间驱动器和硬件设备的驱动程序。

mirror set / 镜像集

数据的完全冗余或阴影副本。镜像集为选定的磁盘提供完全相同的孪生磁盘；写到主磁盘上的所有数据也会写到这个阴影或镜像磁盘。这样，就可以马上访问存有这些信息副本的另一个磁盘。镜像集提供了容错功能。另请参见“带有奇偶校验的带区集”、“卷集”。

mirrored volume / 镜像卷

在两个物理磁盘上复制数据的容错卷。镜像总是位于不同的磁盘上。如果一个物理磁盘发生故障，该磁盘上的数据不再可用，但系统可以使用未受影响的磁盘继续运转。与 RAID-5 卷相比，镜像卷在读取操作时比较慢，但写入操作却更快。镜像卷只能在动态磁盘上创建。在 Windows NT 4.0 中，镜像卷也称“镜像集”。另请参见“动态磁盘”、“动态卷”、“容错”、“独立磁盘冗余阵列 (RAID)”、“卷”。

mixed mode / 混合模式

Windows 2000 域控制器上域的默认模式设置。混合模式允许 Windows 2000 域控制器和 Windows NT 备份域控制器共存于一个域中。 混合模式不支持 Windows 2000 通用和嵌套组增强功能。可以在所有 Windows NT 域控制器从域中删除或升级到 Windows 2000 之后，将域模式设置成 Windows 2000 本机模式。另请参见“本机模式”。

mixed mode domains / 混合模式域

运行了多个操作系统，例如同时有 Windows NT 和 Windows 2000 的联网计算机组。

MMC

请参见“ Microsoft 管理控制台”。

MMC snap-in / MMC 管理单元

一种管理工具，可以把它添加到 MMC 支持的控制台的控制台树，如设备管理器。管理单元可以是独立的，也可以是扩展的。独立管理单元可以自己添加到控制台树；而扩展管理单元却只能添加到其他管理单元来扩展它。另请参见“ Microsoft 管理控制台(MMC) ”。

mobile user / 移动用户

经常离开公司出差的用户，比如销售人员或野外技术人员。

mobility impairments / 行动障碍

执行某些手动操作的能力丧失，比如不能使用鼠标或同时敲击两个键；有些还可能击多个键的倾向或手指回弹；或者不能拿起打印书本。

module / 模块

Windows 2000 操作系统的功能独立的组件。应用程序在独立模块中以用户模式运行，并从中请求系统服务。应用程序进程则被传送到内核模式（受保护的）的一个或多个模块，并在那里得到实际的服务。

MouseKeys / 鼠标键

Microsoft Windows 的一个功能，该功能允许使用数字键盘移动鼠标指针。

mouthstick

一种为有身体残疾者设计的替代辅助输入设备。

MS-DOS-based application / 基于 MS-DOS 的应用程序

设计成在 MS-DOS 上运行的应用程序，因此它可能不能利用 Windows 2000 的所有功能。

multicast / 多播

流向属于多播组的一组主机的网络通信。另请参见“ 多播组 ”。

multicast backbone / 多播骨干网

Internet 的 IP 多播网络部分。

multicast DHCP (MDHCP) / 多播 DHCP (MDHCP)

DHCP 协议标准的一个扩展，它支持基于 TCP/IP 网络上 IP 多播地址的动态分配和配置。

multicast forwarding table / 多播转发表

IP 用来转发 IP 多播通信的表格。IP 多播转发表中的一个项目，它包括多播组地址、源 IP 地址、通信被转发到（后面的跃点接口）的接口列表、和必须接收通信以实现转发的一个接口（前面的跃点接口）。

multicast group / 多播组

一组成员 TCP/IP 主机，它们被配置成负责接听和接收发送到指定目标 IP 地址的数据报。该组的目标地址是一个 D 类地址范围（ 224.0.0.0 到 2239.255.255.255 ）的共享 IP 地址。另请参见“ 数据报 ”。

multicast scope / 多播作用域

239.0.0.0 到 239.254.255.255 内的 IP 多播地址范围。使用基于作用域的多播边界，可以避免该范围内的多播地址向任何方向（发送和接收）传播。

multihomed / 多宿主（计算机）

上面安装多个网卡的计算机。

multilingual APIs / 多语种 API

Windows 2000 中用来支持多种语言的应用程序编程接口。

multimaster replication / 多主控复制

一种复制模式，其中所有域控制器都接受并复制对其它任何域控制器的目录更改。这区别于其它复制模式，有些模式由一台计算机存储目录的一个可修改副本，其它计算机存储目录备份。另请参见“域控制器”、“复制”。

multiple-master replication / 多主控复制

Windows 2000 域控制器控制复制域数据的进程。主域控制器模拟器将域数据复制到其它域控制器。请参见“主域控制器模拟器”。

Multipurpose Internet Mail Extensions (MIME) / 多用途 Internet 邮件扩展 (MIME)

通过 Internet 电子邮件发送非文本数据的常用方法。MIME 将非文本数据编码成 ASCII 文本，并在接收端将其解码回原来的格式。在文件上加上一个 MIME 报头，在此报头里包含数据的的类型和所用编码方法。另请参见“安全/多用途 Internet 邮件扩展 (S/MIME)”。

mutual authentication / 相互身份验证

主叫路由器向应答路由器验证自己的身份，同时应答路由器向主叫路由器验证自己身份的过程。连接的两端都会验证连接另一端的身份。MS-CHAP v2 和 EAP-TLS 身份验证方法提供相互身份验证。

N

name resolution / 名称解析

让软件在名称和数字 IP 地址之间进行转换的过程，名称对于用户容易使用，而 IP 地址对用户来说很难但对 TCP/IP 通讯却是必要的。名称解析可以由一些软件组件提供，如域名系统 (DNS)、Windows Internet 命名服务 (WINS)。在目录服务中，是指 LDAP 目录操作过程的阶段，此阶段查找拥有该操作目标项目的域控制器。另请参见“域名系统 (DNS)”、“传输控制协议/ Internet 协议 (TCP/IP)”、“ Windows Internet 命名服务 (WINS)”。

name resolution service / 名称解析服务

TCP/IP 互连网络将计算机将名称转换成 IP 地址和将 IP 地址转换成计算机名称所需的服务。(人们使用‘友好的”名称来连接计算机；程序则使用 IP 地址。）另请参见“互连网络”、“传输控制协议/ Internet 协议 (TCP/IP)”。

name server / 名称服务器

在 DNS 客户机/服务器模型中，用作 DNS 数据库一部分的服务器。该服务器能提供计算机名称和其它信息，客户解析程序可通过 Internet 或 Intranet 查询名称解析结果。另请参见“域名系统 (DNS)”。

named pipe / 命名管道

一个进程可用来将信息传递到另一个进程的一部分内存，这样一个进程的输出就是另一个进程的输入。第二个进程可以是本地的（和第一个进程在同一计算机上），也可以是远程的（在联网的计算机上）。

namespace / 名称空间

用于共享计算环境的资源或项目的一组唯一名称。名称空间里的名称可被解析成其代表的对象。对于 Microsoft 管理控制台 (MMC)，名称空间用控制台树代表，控制台树显示所有管理单元和控制台能够访问的资源。对于域名系统 (DNS)，名称空间是域名树的垂直或分层结构。例如，在完全合格域名（如 host1.example.microsoft.com）中每个域标签（如 host1 或 example），都指示该域名称空间树的一个分支。对于 Active Directory，名称空间在结构上与 DNS 名称空间相当，但它解析 Active Directory 对象名称。

naming service / 命名服务

一种 WINS 或 DNS 等所提供的服务，它将“友好的”名称解析成地址或其它特殊定义的资源数据。这些地址用来定位不同类型和用途的网络资源。

native mode / 本机模式

域内的所有域控制器都是 Windows 2000 域控制器，并且管理员启用本机模式操作（通过Active Directory 用户和计算机）的情形。另请参见“混合模式”。

nested groups / 嵌套组

Windows 2000 中只在本机模式下可用的一项功能，允许在组内创建其它组。请参见“通用组”、“全局组”、“域本地组”、“目录林”、“信任的目录林”。

NetBIOS Enhanced User Interface (NetBEUI) / NetBIOS 增强型用户接口 (NetBEUI)

Microsoft 网络的一个协议，一般用在有 1 到 200 个客户机的局域网络中。NetBEUI 使用令牌环源路由作为路由唯一方法。它是 NetBIOS 标准的 Microsoft 版本。

NetBIOS name / NetBIOS 名

WINS 识别的名称，该名称与 IP 地址对应。

NetBIOS name resolution / NetBIOS 名称解析

将 NetBIOS 名解析成其 IP 地址的过程。

NetBIOS over TCP/IP (NetBT) / TCP/IP 上的 NetBIOS (NetBT)

在 TCP/IP 协议上提供 NetBIOS 编程接口的功能。它用于监视使用 NetBIOS 名称解析的路由服务器。

Netdom

允许管理 Windows 2000 域和信任命令行关系的工具。

NetWare

Novell 的网络操作系统。

NetWare Core Protocol (NCP) / NetWare 核心协议 (NCP)

文件共享协议，负责管理 Novell NetWare 网络上服务器和客户计算机间资源（如磁盘或打印机）、联编数据库及 NDS 操作的通讯。客户机的请求由 IPX 协议传送。而服务器按照 NCP 原则作出响应。另请参见“联编数据库”、“网际数据包交换 (IPX)”、“Novell 目录服务 (NDS)”。

network adapter / 网卡，网络适配器

将节点或主机连接到局域网的软件或硬件插件板。如果节点是服务器群集的成员，网卡则是服务器群集对象（网络接口对象）。

network address / 网络地址

请参见“网络 ID”。

Network Address Translation (NAT) / 网络地址转换 (NAT)

允许专用地址网络通过 IP 转换进程访问 Internet 信息的协议。

network address translator / 网络地址转换器

RFC 1631 中定义的一个 IP 路由器，能够在转发数据包时转换其 IP 地址和 TCP/UDP 端口号。

network administrator / 网络管理员

负责安装和管理域控制器或本地计算机及其用户和组帐户、分配密码和权限、帮助用户解决网络问题的人员。管理员是管理员组的成员，对域和计算机有着完全控制。

network basic input/output system (NetBIOS) / 网络基本输入/输出系统 (NetBIOS)

可以由应用程序用于局域网或运行 MS-DOS、OS/2、及一些版本的 UNIX 的计算机上使用的应用程序编程接口 (API)。

NetBIOS 为请求底层网络服务提供了一组统一命令。

network gateway / 网关

一种连接使用不同通讯协议的网络，使信息可以在网络间传递的设备。网关在传送信息的同时，还将其转换成与接收网络所用协议兼容的格式。

network ID / 网络 ID

用于标识位于由路由器界定的同一物理网络上的系统的数字。网络 ID 在互连网络中应该是唯一的。

network layer / 网络层

负责为消息寻址、并将逻辑地址和名称转换成物理地址的一层。它还确定从源计算机到目标计算机的路径，管理通信问题比如切换、路由和控制数据包拥塞。

network load balancing / 网络负载平衡

负责将传入的 Web 请求在 IIS 服务器群集中分配的 Windows 群集组件。

network load balancing cluster / 网络负载平衡群集

2 到 32 个 IIS 服务器，网络负载平衡向 Web 客户提供单一 IP 地址，并在 Web 客户中分配传入的 Web 请求。

network media / 网络媒体

用于发送和接收帧的物理布线以及底层协议的类型。例如，以太网、FDDI 和令牌环网络。

Network Monitor / 网络监视器

用于察看网络通信数据包的捕获和分析工具。它是 Windows 2000 Server 包括的一项功能；但 Systems Management Server 中有一更完善的版本。

network name / 网络名称

在服务器群集中，是指客户用来访问服务器群集资源的名称。网络名称类似于计算机名，当在资源组中与客户访问的 IP 地址和应用程序组合时，向客户提供虚拟服务器。

Network News Transfer Protocol (NNTP) / 网络新闻传送协议 (NNTP)

TCP/IP 协议套件中的成员，用于在 Internet 上将网络新闻消息分发给 NNTP 服务器和客户或是新闻读者。设计 NNTP 是因为可以把新闻文章存储在服务器的中心数据库中，让用户能够选择特定的项目阅读。另请参见“传输控制协议 / Internet 协议 (TCP/IP)”

network prefix / 网络前缀

以高序位起始的 IP 网络 ID 中的位数。网络前缀是表示子网掩码的另一种方式。

network prefix notation / 网络前缀符号

将子网掩码以网络前缀表示，而不是用点隔开的十进制符号表示的做法。

NNTP

请参见“网络新闻传送协议”。

node / 节点

在树结构中，指可以在其下面有一个或多个项目与其链接的位置。在局域网 (LAN) 中，是指连接网络并能与其他网络设备进行通讯的设备。在服务器群集中，则指安装了群集服务软件的服务器，它是群集的一个成员。另请参见 LAN。

nonauthoritative restore / 未授权的还原

一种 Windows 2000 域控制器备份副本的还原，其中还原目录中的对象不视为有权限。还原对象会与被还原域的其他副本的更改一起更新。另请参见“授权还原”。

noncontainer object / 非容器对象

在逻辑上不能包含其他对象的对象。文件就是非容器对象。另请参见“容器对象”、“对象”。

nonrepudiation / 认可

一个基本的加密安全功能。认可能保证通讯的一方不能不实地否认已经发生的通讯部分。如果没有认可，有人可能会进行了通讯，然后却否认这些通讯的发生或者声明通讯发生在其它时间。另请参见“加密”、“身份验证”、“保密”、“完整性”。

Novell Directory Services (NDS) / Novell 目录服务 (NDS)

在运行 Novell NetWare 4.*x* 和 NetWare 5.*x* 的网络上，负责维护网络上各种资源的信息，并提供这些资源的访问劝降的一种分布式数据库。

NTFS file system / NTFS 文件系统

一种为使用 Windows NT 和 Windows 2000 特别设计的可恢复文件系统。通过使用数据库、事务处理、和对象范例，NTFS 能提供数据安全性、文件系统可靠性、及其他先进功能。它支持文件系统的恢复、大容量存储媒体和 POSIX 子系统的各种功能。另外，它把所有文件视为有用户定义和系统定义属性的对象，从而支持面向对象的应用程序。

NWLink

网际数据包交换 (IPX)、顺序数据包交换 (SPX) 和 NetBIOS 协议的一种版本，用于 Novell 网络中。NWLink 是一标准网络协议，它支持路由、并支持 NetWare 客户机/服务器应用程序的。那里支持 NetWare 的基于套接字的应用程序与基于 IPX/SPX 套接字的应用程序进行通讯。另请参见“网际数据包交换 (IPX)”、“网络基本输入/输出系统 (NetBIOS)”。

O

object / 对象

用一组不同的、有名字的属性描述的一个项目，比如文件、文件夹、共享文件夹、打印机或者 Active Directory 对象。例如，一个“文件”对象的属性包括它的名称、位置和大小；一个 Active Directory User 对象的属性可能包括这个用户的姓名和 e-mail 地址。当指 OLE 和 ActiveX 对象时，对象还可以是能被链接或嵌入其他对象的任一信息。另请参见“属性”、“容器对象”、“非容器对象”、“父对象”、“子对象”。

object class / 对象类别

对象类别是可以存放在目录中的一个特定类对象的正式定义。对象类别是说明一些具体的事物如用户、打印机或应用程序的一组不同的、有名字的属性。属性包含描述目录对象标识事物的数据。一个用户的属性可能包括这个用户的姓名和 e-mail 地址。术语“对象类别”和“类别”可以替换使用。描述对象的属性是由内容规则确定的。

object linking and embedding (OLE) / 对象链接与嵌入 (OLE)

在应用程序间共享信息的一种方法。将对象比如图形从一个文档链接到其他文档，就是将对象的引用插入到第二个文档。对第一个文档对象的任何更改也会出现在第二个文档中。嵌入一个对象则是将一个对象的副本从一个文档插入到其他文档。对第一个文档的对象的更改不会引起第二个文档更新，除非嵌入对象被显式更新。 另请参见 ActiveX。

offline / 脱机

在服务器群集中，一个资源、组或节点对群集不可用时的状态。资源和组也有脱机状态。另请参见“组”、“节点”、“联机”、“暂停”、“资源”。

OLE

请参见“对象链接与嵌入”。

on-demand installation / “请求”安装

Windows 2000 兼容软件的一个安装选项，它可让用户在首次使用应用程序，而不是首次安装时安装新功能。

on-demand router-to-router VPN connection / “请求”路由器到路由器的 VPN 连接

一种路由器到路由器 VPN 连接，由拥有 Internet 拨号连接的主叫路由器作出。

online / 联机

在服务器群集中，一个资源、组、或节点对群集可用的状态。另请参见“心跳”、“节点”、“脱机”、“暂停”、“资源”。

open database connectivity (ODBC) / 开放式数据库连接 (ODBC)

一个应用程序编程接口 (API)，允许数据库应用程序访问现有不同数据源的数据。

open shortest path first (OSPF) / 开放最短路径优先 （OSPF）

一项用在中型和大型网络中的路由协议。该协议比 RIP 更加复杂，但它在传播路由信息时可以有更好的控制，也更为有效。

organizational units / 部门

域中用到的 Active Directory 容器对象。部门是一些逻辑容器，用户、组、计算机和其他部门可以放入其中。但它只能包含其父域的对象。部门是组策略和委派颁发机构的最小作用域。

original equipment manufacturer (OEM) / 初始设备制造厂家 (OEM)

指设备的制造者。当指制造计算机和计算机相关设备时，初始设备制造厂家一般从其他初始设备的制造厂家购买组件，然后组装成自己的产品。

P

package / 对象包

一个代表嵌入或链接信息的图标。这些信息可以是整个文件，如一个“画图”程序的位图，或者是文件的一部分，如工作簿的单元格。当选中一个对象包时，创建该对象的应用程序会播放此对象（如果是一个声音文件的话），或者打开并显示此对象。如果原始信息做了更改，链接信息也会被更新。但嵌入信息则需要手动更新。在 Systems Management Server 中，是指一个包含将软件分发到分发点的文件和说明的对象。另请参见“嵌入对象”、“链接对象”、“对象链接与嵌入 (OLE)”。

package distribution / 对象包分发

在 Systems Management Server 中，将一个解压缩对象包图像放到分发点、共享此图像及让客户可以访问的过程。这一过程在为对象包指定了分发点时发生。

packet / 数据包

由二进制信息组成的有固定最大大小的传送单元。这一信息提供了数据以及包含 ID 号码、源地址和目标地址及错误控制的报头。

packet filtering / 对象包筛选

防止特定类型的网络数据包被发送或接收。这可以出于安全的考虑（防止未经授权用户的访问），或是禁止不必要的数据包通过慢的连接，提高连接

性能。另请参见“数据包”。

page fault / 页错误

当被请求代码或数据不能放到请求进程可用的物理内存时发生的错误。

page-description language (PDL) / 页描述语言 (PDL)

一种描述打印页面上文本和图像排列方式的计算机语言。另请参见“打印机控制语言 (PCL)”、PostScript。

paging / 页面调度

将虚拟内存在物理内存和磁盘间相互移动的过程。在达到物理内存限制时，页面调度就会发生，但它只针对那些在磁盘空间还没有“备份”的数据。例如，因为文件数据已经在文件系统中分配了磁盘空间，所以不会被调度出去。另请参见“虚拟内存”。

paging file / 页面调度文件

硬盘上 Windows 2000 用来存储没有装入内存的部分程序和数据文件的隐藏文件。页面调度文件和物理内存或 RAM 构成虚拟内存。在需要时，Windows 2000 将数据从页面调度文件移至内存，或从内存移至页面调度文件以为新数据腾出空间。页面调度文件又称为“交换文件”。另请参见 RAM、“虚拟内存”。

parent domain / 父域

对于 DNS 和 Active Directory，是指名称空间树中直接位于其他派生域名（子域）之上的域。例如：reskit.com 是 eu.reskit.com 子域的父域。另请参见“子域”、“域”、“目录分区”。

parent object / 父对象

有其它对象驻留的对象。父对象意味着某种关系。例如，文件夹是一个父对象，而文件或者子对象驻留其中。一个对象可以既是父对象，又是子对象。另请参见“子对象”、“对象”。

parenting / 繁殖

管理一个父域委派和增长到更多子域的的概念，子域由父名导出和委派。另请参见“子域”、“父域”。

partial replica / 部分复制

一种目录分区的只读副本，它包含了这个分区中所有对象的属性的一个子集。在一个目录林中，部分副本的总和称为“全局编录”。在规划中，部分副本的属性被定义为，其中的 attributeSchema 对象已将 isMemberOfPartialAttributeSet 属性设置成 TRUE。另请参见“完全复制”、“全局编录”。

partition / 分区

硬盘的一个逻辑分区。分区可以更方便组织信息。各分区可以格式化成不同的文件系统。一个分区必须在一个物理磁盘上，物理磁盘的主启动记录里的分区表可以包含多达 4 个分区项目。

partition table / 分区表

在主启动记录中计算机用来确定如何访问磁盘的一个区域。对于每个物理磁盘，分区表都可以包含多达四个分区。

password authentication protocol (PAP) / 密码身份验证协议 (PAP)

一个用于验证 PPP 连接的简单明文身份验证方案。用户名和密码由远程访问服务器作出请求，并由远程访问客户以明文格式发回。

path / 路径

一序列目录（或文件夹）名，用于指定目录、文件或文件夹在 Windows 目录树中的位置。路径中的每个目录名和文件名之前都必须有一反斜线 (\)。例如，要指定一个位于 C 盘驱动器上 Windows 目录中名为 Readme.doc 的文件的路径，您可以键入 C:\Windows\Readme.doc。

paused / 暂停

节点作为在服务器群集中完全活跃的成员，但不能作为组的主机的状态。提供暂停状态是为了让管理员执行维护工作。另请参见“群集成员”、“故障回复”、“故障转移”、“节点”、“脱机”。

PC Card / PC 卡

一种可移动设备，可以插入便携式计算机的 PCMCIA（个人计算机存储器卡国际协会）插槽，大约有信用卡大小。PCMCIA 设备包括调制解调器、网卡和硬盘驱动器。

performance counter / 性能计数器

系统监视器中与性能对象关联的一个数据项目。对于每个选中的计数器，系统监视器都会提供一个与性能对象某个特定方面的性能相对应的值。另请参见“性能对象”。

performance object / 性能对象

系统监视器中计数器的一个逻辑集合，与能被监视的一个资源或一项服务相关联。另请参见“性能计数器”。

peripheral component interconnect (PCI) / 外设部件互连总线 (PCI)

一项由 Intel 公司引入的规范，定义了一种本地总线系统，允许在计算机上安装多至 10 个 PCI 兼容的扩展卡。

permanent virtual circuit (PVC) / 永久虚电路 (PVC)

分配给预配置静态路由的虚电路。

permission / 权限

一条与对象关联的规则，用来控制哪些用户可以何种方式访问这些对象。Windows 2000 中，对象包括文件、文件夹、共享设备、打印机和 Active Directory 对象。Macintosh 服务在权限和 Macintosh 访问特权间进行翻译，这样，设置在文件夹（卷）上的权限会被加给 Macintosh 用户，而由 Macintosh 用户设置的访问特权也被加给连接到运行 Windows 2000 Server 的计算机的个人计算机用户。另请参见“对象”。

personal identification number (PIN) / 个人识别码 (PIN)

一个机密标识代码，用于保护智能卡不被错用。PIN 和密码相似，只有卡所有者才知道。智能卡也只有那些拥有它并知道 PIN 的人才可以使用。另请参见“智能卡”。

ping

一个用来验证与一个或多个远程主机连接的工具。ping 命令使用 ICMP 回送请求和回送答复数据包来确定网络上的一个 IP 系统是否能用。Ping 在诊断 IP 网络和路由器故障时很有用。 另请参见“网际消息控制协议 (ICMP)”。

plaintext / 明文

指未加密的数据。有时也叫作“明码电文”。另请参见“暗记文”、“加密”、“解密”。

Plug and Play / 即插即用

一组由 Intel 开发的规范，允许计算机自动检测和配置设备并安装合适的设备驱动程序。

Point-to-Point Protocol (PPP) / 点对点协议 (PPP)

一个行业标准协议组，用于点对点链接传输多协议数据报。PPP 在 RFC 1661 中有记录。

Point-to-Point Tunneling Protocol (PPTP) / 点对点隧道协议 (PPTP)

一项将点对点协议 (PPP) 帧压缩成 IP 数据报，并通过基于 IP 的互连网络如 Internet 和专用 intranet 传送的隧道协议。

port / 端口

一个允许多个会话的装置。是一个 IP 地址的固化。在设备管理器中，是指计算机上数据传出和传入设备的连接点。例如，打印机一般连接到并口（也就是 LPT 端口），调制解调器则一般连接到串口（也就是 COM 端口）。

port rule / 端口规则

对于网络负载平衡，是指确定一系列端口筛选模式的一组配置参数。另请参见“筛选模式”。

PostScript

Adobe Systems 为激光打印机打印开发的一种页描述语言 (PDL)。PostScript 可以提供灵活的字体性能和高质量的图形。它是桌面出版的标准，因为图像设备、商用类型的打印服务用到的高分辨率打印机都支持它。另请参见“打印机控制语言 (PCL)”、“页描述语言 (PDL)”。

primary domain controller / 主域控制器

一个 Windows NT 4.0 和 3.51 域控制器，在域中被首先创建，并包含了域数据的主仓库。在域中，主域控制器定期将其数据复制到另一域控制器，即备份域控制器。另请参见“备份域控制器”。

primary domain controller emulator / 主域控制器模拟器

在域中创建的第一个 Windows 2000 域控制器。除了将域数据复制到其他 Windows 2000 域控制器，主域控制器模拟器还象 Windows NT 主域控制器那样执行主域控制器的职责，包括将域数据复制到域中的任一备份域控制器。主域控制器模拟器脱机时，域中另一个 Windows 2000 域控制器会充当主域控制器模拟器的角色。另请参见“主域控制器”、“备份域控制器”。

primary partition / 主分区

一个在基本磁盘上用未分配空间创建的卷。Windows 2000 和其它操作系统可以从主分区启动。在一个基本磁盘上最多可以创建四个主分区，或者三个主分区加一个扩展分区。主分区只能在基本磁盘上创建，且不能再被分区。另请参见“基本磁盘”、“动态卷”、“扩展分区”、“分区”。

primary server / 主服务器

一个可用作区域更新点的授权 DNS 服务器。只有主服务器才能直接更新以实现区域更新，区域更新包括添加、删除或修改存为区域数据的资源记录。主服务器也是将区域复制到其他 DNS 服务器的首选源。

primary token / 主令牌

一个分配给进程的访问令牌，代表该进程的默认安全信息。它是由代表进程本身的而不是代表客户的线程在

安全操作中使用。另请参见“访问令牌”、“模拟令牌”、“进程”。

print device / 打印设备

一种用于打印的硬件设备，通常称为打印机。另请参见“逻辑打印机”。

print server / 打印服务器

专门用于管理网络打印机的计算机。打印服务器可以是网络上的任一计算机。

print sharing / 打印共享

运行 Windows NT Workstation 或 Windows NT Server 的计算机可以共享网络上打印机的功能。这可以通过双击“控制面板”中的“打印机”，或者在命令提示符后输入网络共享命令实现。

print spooler / 打印后台处理程序

负责接受用户发送到打印机的文档，然后将其存到磁盘或内存，直到打印机准备好的软件。这个动态链接库 (DLL) 的集合会接收、处理、安排和分配需要打印的文档。术语 spooler（假脱机程序，后台程序）是 simultaneous print operations on line（联机同步打印操作）的首字母缩写。另请参见“后台打印”。

printer control language (PCL) / 打印机控制语言 (PCL)

Hewlett Packard 为其激光和喷墨打印机开发的页描述语言 (PDL)。由于激光打印机的广泛使用，这种命令语言已成为很多打印机的标准。另请参见“页描述语言 (PDL)”、PostScrip。

printer driver / 打印机驱动程序

为其它程序使用特定打印机而设计的程序，通过它就不用考虑打印机本身的硬件和内部语言细节。由于打印机驱动程序处理各个打印机的细微之处，其他程序就能与不同类型的打印机正常对话。另请参见“打印机控制语言 (PCL)”、PostScript。

printer permissions / 打印机权限

一些指定用户或组对打印机访问类型的权限。打印机权限包括“打印”、“管理打印机”和“管理文档”。

printers folder / 打印机文件夹

“控制面板”中的一个文件夹，包含了“添加打印机”向导和所有安装在计算机上的打印机的图标。

priority / 优先级

一个确定进程的各线程使用处理器顺序的优先权排名。

private addresses / 专用地址

专用地址空间中的一些 IP 地址，为各单位的专用 Intranet 寻址而设计。专用 IP 地址可以在以下地址段内：10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

private key / 私钥

密钥对中不公开的一半，和公钥算法一起使用。私钥一般用于数据的数字签名，及对使用相应的公钥加密的数据进行解密。另请参见“公钥”。

privilege / 特权

用户执行特定任务的权利。一般来说，它作用于整个计算机系统而不是特定的对象。管理员给个人用户或用户组分配特权是计算机安全设置的一部分。另请参见“ 访问令牌 ”、“ 权限 ”、“ 用户权力 ”。

process / 进程

由一个可执行程序、一组虚拟内存地址及一个或多个线程组成的操作系统对象。当程序运行时，就会产生一个 Windows 2000 进程。另请参见“ 线程 ”。

protocol / 协议

一组用于网络上两台计算机间消息传递的规则和约定。网络软件通常执行了多层协议。这些协议一层在一层之上。Windows NT 和 Windows 2000 包括 NetBEUI、TCP/IP 和 IPX/SPX 兼容协议。

public addresses / 公用地址

一些由 Internet 网络信息中心 (InterNIC) 分配的IP 地址，它们是全球唯一的并可通过 Internet 连接。

public key / 公钥

密钥对中公开的一半，和公钥算法一起使用。公钥一般用于验证数字签名，及对使用相应的私钥加密的数据进行解密。另请参见“ 私钥 ”。

public key certificate / 公钥证书

一个用作身份证明的数字护照。公钥证书是由证书颁发机构 (CA) 颁发的。另请参见“ 证书颁发机构 (CA) ”、“ Kerberos 协议 ”。

public key cryptography / 公钥密码系统

一种加密方法，在其中使用两个不同的密钥。即，用于加密数据的公钥和用于解密数据的私钥。公钥加密也称为“ 不对称加密 ”。

public key infrastructure / 公钥基础结构

管理和处理证书及公私钥的一些法律、政策、标准和软件。在实践中，它是由验证电子交易各方的合法性的数字证书、证书颁发机构和其它注册机构组成的系统。尽管它们作为电子商务的必要要素正得到广泛应用，PKI 标准仍在不断发展。

public/private key pair / 公/私钥对

公钥加密中用到的一组密钥。其中，一个用于加密，另一个用于解密。另请参见“ 公钥 ”、“ 私钥 ”。

published applications / 已发行应用程序

组策略对象管理的用户可以使用的应用程序。使用“ 控制面板 ”中的“ 添加/删除程序 ”，用户就可以决定是否要安装已发行应用程序。

pull partner / “ 拉 ”伙伴

Windows Internet 命名服务 (WINS) 中的一项服务，通过请求并接受“ 推 ”来的副本，将副本从“ 推 ”伙伴“ 拉 ”回。另请参见“ 推 ”伙伴。

push partner / “ 推 ”伙伴

Windows Internet 命名服务 (WINS) 中的一项服务，在接收到“ 拉 ”伙伴的请求后，将副本发送给“ 拉 ”

伙伴。另请参见“拉”伙伴。

Q

QoS Admission Control Service / QoS 许可控制服务

一种软件服务，负责在被分配到的子网上控制带宽和网络资源。它将为重要的应用程序分配较多的带宽，而相对不重要的应用程序则带宽较少。QoS 许可控制服务可以被安装到任何运行 Windows 2000 的联网计算机上。

Quality of Service (QoS) / 服务质量(QoS)

一套在 Windows 2000 中实现的保证数据传输质量的标准和机制。

queue / 队列

等待执行的程序或任务的列表。在 Windows 2000 的打印术语中，队列指一组等待打印的文档。在 NetWare 和 OS/2 环境中，队列是应用程序和打印设备之间的基本软件接口；用户向队列提交文档。然而在 Windows 2000 中，打印机就是这个接口；文档不再被提交到队列，而是发送到打印机。

quorum log / 仲裁日志

它存储于仲裁磁盘上，记录了上一次配置单元检查点以后，对注册表的群集配置单元所作的更改。也称故障恢复日志或更改日志。

R

RAID / 独立磁盘冗余阵列

另请参见“独立磁盘冗余阵列”。

RAID-5 volume / RAID-5 卷

一种容错卷，数据和奇偶校验的带区间隔分布于三个或更多物理磁盘之上。奇偶检验值由计算得出，用于在故障发生后重建数据。如果物理磁盘的一部分发生故障，用户可以根据其余的数据和奇偶校验重建故障部分的数据。

RAM / 随机访问存储器

另请参见“随机访问存储器”。

raster fonts / 光栅字体

存储为位图的字体，又称位图字体。光栅字体为特定的打印机而设计，有特定大小和分辨率，不能缩放和旋转。不支持光栅字体的打印机无法打印该字体。

read-only memory (ROM) / 只读存储器

包含不可修改的信息的半导体电路。

recovery / 故障恢复

系统崩溃后，通过日志文件将数据库还原为连贯的状态的过程，以及在媒体故障后，从备份中把数据库还原到日志文件中记载的最近状态的过程。另请参见“授权还原”。

redirection / 重定向

在 UNIX 中，将标准输出发送到一个文件（而不发送到终端），或是从一个文件（而不是从终端)获得标准输入。

redirector / 重定向器

另请参见“ Windows 2000 重定向器 ”。

redundant array of independent disks (RAID) / 独立磁盘冗余阵列（RAID)

一种将容错磁盘系统标准化和进行分类的方法。它有六个等级，评估不同的性能、可靠性和成本的组合。Windows 2000 提供了三个 RAID 等级：等级 0（带区）、等级 1（镜像）和等级 5（带有奇偶校验的带区集）。另请参见“ 容错 ”、“ 镜像卷 ”、“ RAID-5 卷 ”和“ 带区卷 ”。

referral / 引用

在 Dfs 中，用来把逻辑名称空间中的 DNS 名映射到物理共享的 UNC 等价名称的信息。当 Dfs 客户访问 Dfs 名称空间中的共享文件夹时，Dfs 根目录服务器将为该客户返回一个引用，用以定位这个共享文件夹。DNS 中指向一个权威 DNS 服务器的指针，该服务器对于低等级的域名空间来说是权威的。

refresh / 刷新

以当前的数据更新显示信息。

refresh interval / 刷新间隔

在 DNS 中，刷新区域数据之前需要经过一段 32 位时间间隔。在刷新间隔期满之后，辅助服务器将使用该区域的主服务器检查自己的区域数据是否是当前的最新数据，是否需要使用区域复制来更新数据。这一间隔在每个区域的起始颁发机构（SOA）资源记录中设置。另请参见“ 资源记录 ”、“ 辅助服务器 ”、“ 起始颁发机构（SOA）资源记录 ”、“ 区域 ”和“ 区域复制 ”。

refresh rate / 刷新速率

指显示屏为防止图象闪烁的回描频率。大多数监视器的整个图象区域以大约每秒 60 次的频率刷新。

registry / 注册表

在 Windows 2000、Windows NT 和 Windows 98 中的关于计算机配置的信息数据库。注册表按层次结构组织，并由子树及其注册表项、配置单元和项目组成。

registry key / 注册表项

注册表中记录或记录组的标识符。

relative identifier (RID) / 相对标识符（RID)

指安全标识符（SID) 中标识帐户或组的部分。RID 相对于创建该帐户或组的域来说是唯一的。另请参见“ 安全标识符 ”。

remote access policy / 远程访问策略

一组条件和连接参数，定义传入连接的特性以及施加于其上的一组限制。远程访问策略确定是否接受授权某一特定的连接尝试。

remote access server / 远程访问服务器

一台基于 Windows 2000 Server 的计算机，运行路由和远程访问服务，并被配置为提供远程访问。

Remote Access Service (RAS) / 远程访问服务

一种 Windows NT 4.0 服务，为远程通勤人员、工作位置不固定的人员，以及监视和管理多个办公室中服务器的系统管理员提供远程联网。

remote computer / 远程计算机

一台只能通过通信线路或通信设备（网络适配器、调制解调器等）访问的计算机。

remote installation boot floppy (RBFG.exe) / 远程安装启动软盘 (RBFG.exe)

远程安装服务中的组件，它创建一张启动软盘，用于在特定的客户计算机上安装基于 RIS 的操作系统。

Remote Installation Preparation wizard / 远程安装准备向导 (RIPrep.exe)

远程安装服务中的组件，用于创建操作系统映象并把它们安装到 RIS 服务器。

Remote Installation Services (RIS) / 远程安装服务 (RIS)

Windows 2000 的一个可选组件，用于远程安装 Windows 2000 Professional。它通过将计算机连接到网络，在启动客户计算机后用有效的用户帐号登录，将操作系统安装到远程可启动的客户计算机。

Remote Installation Services setup (RISetup.exe) / 远程安装服务安装程序 (RISetup.exe)

远程安装服务中的组件，用于安装 RIS 服务器。

remote procedure call (RPC) / 远程过程调用 (RPC)

一个消息传递工具，允许分布式应用程序调用网络中各台计算机上的可用的服务。在计算机的远程管理中使用。

remote storage / 远程存储

对于 Windows 2000 服务器来说，是指在库中用作辅助数据存储设备的可去除的磁带。指定作为辅助数据存储设备的磁带由“ 远程存储 ”管理，并包含本地存储设备上的数据或已经从本地存储设备上去除以释放磁盘空间的数据。另请参见“ 本地存储 ”。

repackaging / 重新包装

指转换较陈旧的应用程序的过程，这样就可以利用许多 Windows Installer 特性，包括向用户公布应用程序的能力、软件在关键文件被删除或损坏时能够修复自身的能力以及用户能够以提高后的特权安装应用程序的能力。

RepeatKeys / 重复键

指允许用户能够通过减少灵活度来调整重复率或禁用键盘的键重复功能的特性。

replica / 副本

在 Active Directory 复制中，通过在持有同一目录分区的副本的域控制器之间进行复制来实现同步的逻辑 Active Directory 分区的副本。副本也可以指任何一个域控制器持有的目录分区的合集。

replication / 复制

把数据从一个数据存储载体或文件系统复制到多台为数据同步的目的而存储有相同的数据的计算机的过程。在 Windows 2000 中，Active Directory 的复制通过“ 目录复制程序服务 ”进行，而文件系统的复制通过 Dfs 复制来进行。

replication latency / 复制潜伏期

指在 Active Directory 复制中，更新被应用到某一目录分区的给定副本的时间和更新被应用到同一目录分区的其它某个副本的时间之间的延迟。潜伏期有时指传播延迟。另请参见“ 多主控复制 ”。

replication topology / 复制拓扑

指在 Active Directory 复制中，域控制器用来在它们之间复制信息的连接的集合，复制可能在站点内或站点间进行。另请参见“ 域控制器 ”、“ Active Directory 复制 ”。

Request for Comments (RFC) / 注释请求

定义 TCP/IP 标准的文档。RFC 由“ 因特网工作部 (IETF) ”及其它工作组出版。

resolver / 解析器

用来查找 DNS 名信息的 DNS 客户程序。解析器可以是一个小的“ 存根 ”（一个有限的提供基本查询功能的常规程序集合），也可以是一些能够提供额外的 DNS 客户查询功能，如缓存等，的较大的程序。另请参见“ 缓存 ”、“ 缓存解析器 ”。

resource / 资源

计算机系统或网络的任何能够被分配给运行中的程序或进程的部分，如磁盘驱动器、打印机或存储器等。对于“ 设备管理器 ”来说，是指四个控制计算机上设备工作方式的组件中的任何一个。这四个系统资源是：中断请求 (IRQ) 线路、直接内存访问 (DMA) 信道、输入/输出 (I/O) 端口以及内存地址。另请参见“ 直接内存访问 (DMA) ”、“ 输入/输出断口 ”、“ 中断请求 (IRQ) 线路 ”和“ 内存地址 ”。在服务器群集中，是指一个资源类型的范例；群集服务以资源的形式管理各种物理或逻辑的项。

Resource DLL / 资源 DLL

指为某一特定资源类型定义默认属性和行为的动态链接库。“ 资源 DLL ”包含某一特定资源类型的“ 资源 API ”的实现，并被加载到它的“ 资源监视器 ”的地址空间。另请参见“ 动态链接库 ”和“ 资源监视器 ”。

resource domain / 资源域

指拥有工作站和资源计算机（例如：文件和打印服务器）的帐户数据的 Windows NT 域，并带有帐户或主域。另请参见“ 帐户域 ”、“ 主域 ”。

Resource Monitor / 资源监视器

指管理在节点的群集服务和它的一个或多个资源之间的通信的服务器群集组件。另请参见“ 节点 ”、“ 资源 ”

resource record / 资源记录 (RR)

DNS 数据库中用来处理客户查询的信息。每一个 DNS 服务器都包含有它需要的资源记录，用来回答关于该服务器是权威的那部分 DNS 名称空间的查询。

response time / 响应时间

从工作开始到完成所需要的时间。在客户/服务器环境中，该时间通常在客户端测量。

reverse lookup / 反向搜索

一个使用 IP 地址来确定计算机的 DNS 名的查询。

reverse lookup zone / 反向搜索区域

包含有执行反向搜索所必须的信息的区域。另请参见“ 反向搜索 ”。

roaming profile / 漫游配置文件

在一台服务器上的单一位置上的一组用户相关的设置，使得用户在计算机之间移动的同时能够保持配置文件不变。

roaming user profile / 漫游用户配置文件

当用户登录时下载到本地计算机上的基于服务器的用户配置文件，当用户注销时本地计算机和服务器的配置文件都得到更新。当用户登录到任何运行 Windows 2000 Professional 或 Windows 2000 Server 的计算机上时漫游用户配置文件都在服务器上可用。在登录时，如果本地配置文件比在服务器上的副本更新的话，则用户可以使用本地用户配置文件。

root / 根

在分层组织的信息集合中的最高或最上一层。根是指这样一个点，从该点开始的进一步的子集以一种逻辑的顺序分叉，这种逻辑的顺序沿着更宽广或更一般性的视角变化到更窄的视角。

root certificate / 根证书

一个自签名的证书颁发机构证书。因为它是根颁发机构的证书，所以它被称作根证书。根颁发机构必须对它自己的证书签名，因为在证书等级中再也没有更高的认证机构了。另请参见“ 证书 ”、“ 证书颁发机构 ”和“ 根颁发机构 ”。

root certification authority / 根颁发机构

最可信的证书颁发机构 (CA)，位于证书等级的顶层。根 CA 拥有自签名的证书。又称作根颁发机构。另请参见“ 证书颁发机构 “ 、证书路径 ”和“ 根证书 ”。

root domain / 根域

域名系统 (DNS) 名称空间的初始域。在 Active Directory 中是一棵 Active Directory 目录树的初始域。也是一个目录林的初始域。

round robin / 循环共享

DNS 服务器使用的一种简单的机制，用来为网络资源共享和分配负载。 循环共享用于在对于一个查询的 DNS 域名的 RR 类型存在多个 RR 时旋转在一次查询应答中返回的资源记录 (RR) 数据的顺序。

route summarization / 路由总结

把多个网络 ID 结合成为路由表中的一条单独的路由的过程。有了正确的规划，分层的路由基础结构就能使用路由总结。

router / 路由器

一个网络服务器，用于帮助 LAN 和 WAN 实现互操作和互连并能链接拥有不同网络拓扑的 LAN，如 Ethernet 和“令牌环”等。

routing / 路由选择

基于目的 IP 地址转发数据包的过程。

routing infrastructure / 路由基础结构

Internet 网络的结构和拓扑。

routing protocol / 路由协议

一系列周期的或请求的包含路由信息的消息，这些消息在路由器之间交换路由信息并提供容错。除了在初始配置时，动态路由器只需要很少的运行间维护，因此就可以被扩展应用于较大的互连网络。

routing table / 路由表

路由数据库，包含有关于网络 ID、转发地址和互连网络上可到达网段的指标的信息。

rules / 规则

一种 IPSec 策略机制，用来规定 IPSec 策略如何及何时保护通信。提供触发和控制基于源、目标和 IP 通信类型的安全通信的能力的规则。每一条规则包含一个 IP 筛选器列表和在这个筛选器列表上发生的安全操作的集合。

S

scalability / 可扩展性

一种关于某一计算机、服务或应用程序能够在多大程度上扩展以满足不断增长的性能要求的量度。对于服务器群集来说，是指当群集的总负载超过了它的负载能力时，增量添加一个或多个系统到这个现存的群集中的能力。

scaling / 扩展

向系统添加处理器以实现更高的吞吐量的过程。

schema / 方案

对存储在 Active Directory 中的对象类和属性的描述。对于每个对象类来说，方案定义了一个对象类必须有哪条属性、可以有哪条附加属性以及哪个对象类可以是它的父类。Active Directory 方案可以被动态更新。例如：一个应用程序可以用新的属性和类来扩展方案，并立即使用扩展的部分。方案更新是通过创建或修改存储在 Active Directory 中的方案对象来完成的。如同在 Active Directory 中的每一个对象一样，方案对象有一个访问控制列表，从而使得只有经过授权的用户才能修改方案。

script / 脚本

一种程序，由一组对某一应用程序或实用程序的说明组成。脚本通常使用应用程序或实用程序的规则或语法，并结合如循环和 if/then 表达式等简单的控制结构来表示说明。在 Windows 环境下批处理程序通常可以与脚本互换使用。

secondary server / 辅助服务器

指某一区域的权威 DNS 服务器，用作该区域到其它服务器的复制的源。辅助服务器只通过从其它 DNS 服务器传输区域数据来更新它们的区域数据，而没有执行区域更新的能力。另请参见“ 主服务器 ”和“ 区域复制 ”。

secondary storage / 辅助存储器

用来存储从管理的卷中迁移出的数据的存储设备。辅助存储器包括硬盘上用作数据分步迁移区的那一部分。

secret key / 秘密密钥

仅在两个通信方之间共享的加密密钥。另请参见 “ 对称密钥加密 ”。

secure dynamic update / 安全动态更新

安全动态更新客户向 DNS 服务器提交动态更新请求的过程，只有当该客户能够证明他的身份并拥有正确的凭据的时候该服务器才会尝试执行更新操作。另请参见 “ 动态更新 ”。

Secure Sockets Layer (SSL) / 安全套接字层 (SSL)

Netscape Communications 开发并提出的为建立安全通信信道以防止对如信用卡号等关键信息的截取的开放标准。它主要使得在“ 万维网 ”上进行安全的电子财政事务成为可能，尽管它被设计成也可以在其它 Internet 服务上工作。

Secure/Multipurpose Internet Mail Extensions (S/MIME) / 安全/多用途 Internet 邮件扩展

MIME 的扩展， 用来支持安全邮件。它使得消息的发起者可以对电子邮件消息进行数字签名，从而提供了对于消息来源和数据完整性的证据。它还使得可以以加密的格式传输消息，从而提供了保密通信的能力。另请参见 “ 多用途 Internet 邮件扩展 (MIME) ”。

security administrator / 安全管理员

被分配了管理审核和安全日志的权限的用户。默认时，该用户权限被授予 Administrators 组。另请参见 “ 审核 ”、“ 系统访问控制列表 (SACL) ”和 “ 用户权限 ”。

security association (SA) / 安全关联 (SA)

一组参数，用来定义保护 Internet 协议安全通信所必需的服务和机制。另请参见 “ Internet 协议安全 (IPSec) ”。

security context / 安全上下文

当前起作用的安全属性或规则。例如：规定用户可以对一个受保护的对象做什么的规则由用户的访问令牌和对象的安全描述符中的安全信息所确定。访问令牌和安全描述符一起构成了用户在对象上的操作的安全上下文。另请参见 “ 访问令牌 ”和 “ 安全描述符 ”。

security descriptor / 安全描述符

某一对象附属的一组信息，用来描述赋予用户、组以及被审核的安全事件的权限。另请参见 “ 任意访问控制表 (DACL) ”、“ 对象 ”和 “ 系统访问控制列表 (SACL) ”。

security groups / 安全组

能够被用来管理用户和其它域对象的权限的组。

security identifier (SID) / 安全标识符 (SID)

用来标识某一登录到 Windows NT 或 Windows 2000 安全系统中的用户的唯一名称。安全标识符可以代表某一个人用户、一组用户或者一台计算机。

security method / 安全措施

一个用来确定在通信中将被用来保护数据到的 Internet 协议安全服务、密钥设置和算法的过程。

security principal / 安全负责者

一个 Windows 2000 实体，它被自动分配了一个用来访问资源的安全标识符。安全负责者可以是一个用户、组或计算机。Windows 2000 使用 Active Directory 来对用户和安全负责者进行帐户管理。另请参见“ 安全负责者名称 ”。

security principal name / 安全负责者名称

在某个单独的域中唯一地标识一个用户、组或计算机的名称。该名称在域之间并不一定是唯一的。另请参见“ 安全负责者 ”。

seek time / 寻找时间

磁盘头把自身定位到正确的柱面以存取请求的数据所需要的时间。

sender / 发件人

使用已经存在的连接系统在站点之间通信的“ 系统管理服务器 ”线程组件。发件人管理连接，确保传送的数据的完整性，从错误中恢复，并当不再需要使用连接时关闭连接。

SerialKeys / 串行键

一种 Windows 的特性，它使用通信辅助接口设备来允许通过计算机串行端口接受按键和鼠标控制。

server / 服务器

一台为网络用户提供共享资源的计算机。

server cluster / 服务器群集

指由群集服务和相关的软件（.exe 和 .dll 文件）创建和管理的群集，在它的节点之间群集服务为在服务器上运行的应用程序提供故障转移支持。服务器群集包括硬件和群集配置以及群集服务。另请参见“ 群集 ”和“ 节点 ”。

server message block (SMB) / 服务器消息块 (SMB)

一种文件共享协议，设计用来使得联网的计算机能够通过多种网络透明地访问位于远程系统之上的文件。SMB 协议是由 Microsoft、Intel 和 IBM 共同开发的，它定义了一系列能够在计算机之间传递信息的命令。SMB 使用四种消息类型：会话控制、文件、打印机和消息。

service level agreement (SLA) / 服务等级协议 (SLA)

用户的 IT 组和另外一些用户之间的协定，这些用户指定哪些性能等级对于如设备替换、网络当机时间等服务来说是可以接受的。

service name / 服务名称

通过该名称用户就可以知晓一个端口。

service ticket / 服务票据

请参见“ 会话票据 ”。

session key / 会话密钥

主要用于加密和解密的密钥。会话密钥通常与对称加密算法一起使用，在对称加密算法中加密和解密使用相同的密钥。由于这个原因，会话密钥和对称密钥通常指同一种类型的密钥。另请参见“ 对称密钥加密 ”。

session ticket / 会话票据

在 Kerberos 身份验证协议中客户向服务出示的凭据。因为会话票据用于获得到服务的已验证连接，所以它们有时也被称作服务票据。另请参见“ Kerberos 身份验证协议 ”、“ 密钥分发中心 (KDC) ”。

sessions / 会话

在两个终结点之间发送的带有确认的多个数据包。

shared printer / 共享打印机

接收来自多台计算机的输入的打印机。例如：连接到网络上的另一台计算机的打印机可以被共享使用，从而许多用户都可以使用这台打印机。又叫做网络打印机。

shell / 外壳

用来把命令传递给操作系统的命令解释程序。

shortcut trust / 快捷方式信任

一种双向的信任关系，显式地创建于一个目录林的不同的域目录树中的两个 Windows 2000 域之间。快捷方式信任的目的是优化域间身份验证过程。快捷方式信任只能创建于同一目录林的 Windows 2000 域之间。所有的快捷方式信任都是可传递的。另请参见“ 域目录树 ”、“ 目录林 ”和“ 可传递信任 ”。

ShowSounds / 声音显示

一个全局标志，用于引导程序显示所发出的语音和系统声音的文字来提醒那些有听力缺陷的用户或在如工厂车间等极为嘈杂的环境中工作的用户。

Simple Mail Transport Protocol (SMTP) / 简单邮件传输协议 (SMTP)

在 Internet 上用来可靠和高效地传输邮件的协议。SMTP 独立于特定的传输子系统，并只需要一条可靠的、有序的数据流信道。

Simple Network Management Protocol (SNMP) / 简单网络管理协议 (SNMP)

一种与 TCP/IP 一起安装的网络管理协议，广泛使用于 TCP/IP 和“ 网际信息包交换 (IPX) ”网络之上。SNMP 在由管理员运行的管理程序和某台主机上运行的网络管理代理之间传输管理信息和命令。当主机请求时，或有重要事件发生时，SNMP 代理发送状态信息到一台或多台主机

single point of failure / 单点故障

指用户环境中的任何在发生故障时会阻塞数据或应用程序的组件。

site / 站点

网络中的一个拥有 Active Directory 服务器的位置。一个站点被定义为一个或多个良好连接的 TCP/IP 子网。（“良好连接”在这里意味着网络连接是高度可靠和快速的。）因为从网络的角度来看同一站点中的计算机相互之间是非常接近的，

END BREAK

因此它们之间的通信是可靠、快速和高效的。把站点定义为一组子网的集合，这就允许管理员配置 Active Directory 访问和复制的拓扑以利用物理网络的优点。当用户登录到网络上的时候，Active Directory 客户以客户的身份在同一站点中找到 Active Directory 服务器。在“系统管理服务器”中，站点服务器和客户计算机由一组子网限制，如 IP 子网和 IPX 网络号等。另请参见“域控制器定位器”、“子网”和“复制拓扑”。

site server / 站点服务器

一台运行 Windows NT Server 的服务器，在其上还运行了“系统管理服务器 (SMS)”站点安装程序。当一台计算机上安装了 SMS 之后，这台计算机就已经被分配了站点服务器的角色。站点服务器，作为监视和管理一个 SMS 站点所需要的 SMS 组件的主机，通常拥有几个附加的 SMS 角色，包括组件服务器、客户访问点和分配点。

slow link processing / 慢速连接处理

一种可配置的“组策略”处理模式，它允许管理员定义在慢速网络链接上哪些组策略将不被处理。

SlowKeys / 慢键

一种 Windows 的特性，用来引导计算机忽略那些按住的时间没有达到最小时间限制的按键，这使得用户可以滑过按键而没有任何影响。另请参见“筛选键”。

Small Computer System Interface (SCSI) / 小型计算机系统接口 (SCSI)

一种标准的高速并行接口，由美国国家标准学会 (ANSI) 的 X3T9.2 委员会定义。SCSI 接口用于把微型计算机连接到如硬盘和打印机等外围设备，或连接到其它计算机和局域网。

Small Office/Home Office (SOHO) / 小办公室 / 家居办公室 (SOHO)

一个拥有一些计算机的办公室，且这些计算机能够被看作一个小型商务或某个较大网络的一部分。

smart card / 智能卡

一个信用卡大小的设备，带有一个提供基于证书的身份验证功能的 PIN 序号以及一条单独的到企业的开始指令。智能卡能够安全地存储证书、公钥和私钥、口令以及其它类型的个人信息。智能卡读取器附属于读取智能卡的计算机。另请参见“身份验证”。

smart-card reader / 智能卡读取器

一种安装到计算机内部的设备，使得利用智能卡来增强安全特性成为可能。另请参见“智能卡”。

SMTP 协议

请参见“简单邮件传输协议”。

sniffer / 监探器

一个能够读取、监视和捕获网络数据交换并读取网络数据包的应用程序。如果这些网络数据包没有加密，则

监探器就可以全面观察数据包内部的数据。

SOA (start of authority) resource record / SOA（起始颁发机构）资源记录

请参见“ 起始颁发机构（SOA）资源记录 ”。

software inventory / 软件清单

在“ 系统管理服务器“ 中，SMS 用来搜集关于客户计算机上软件的信息的自动化过程。

software metering / 软件监测

在“ 系统管理服务器 ”中，SMS 用来监视和管理软件应用程序使用以确保其遵循软件授权协议或了解软件用法的过程。

SoundSentry / 声音卫士

一种 Windows 特性，用来产生可视的提示以代替系统声音，如屏幕闪烁或闪烁的标题栏等。

speech synthesizer / 语音合成器

一种产生话语的辅助设备，这可以通过结合预先录制好的单词来实现，也可以通过对计算机进行编程以产生能够组成话语的声音来实现、

spooling / 后台打印

服务器上的进程，这种进程中在打印机准备好处理带打印的文档之前，它们先被存储在磁盘上。后台打印程序从用户那里接收文档、存储并在打印机准备好时将它们发送给打印机。

stand-alone certification authority / 独立证书颁发机构

未与 Active Directory 结合在一起的 Windows 2000 证书颁发机构。另请参见“ 证书颁发机构 ”和“ 企业证书颁发机构 ”。

start of authority (SOA) resource record / 起始颁发机构 (SOA) 资源记录

为存储在某区域内的信息指示颁发机构的起始点或初始点的记录。SOA 资源记录（RR）是当添加一个新区域时创建的第一个 RR。它还包含几个参数，其它记录用这几个参数来确定其它 DNS 服务器能够使用该区域的信息多长时间及过多久就需要更新一次。另请参见“ 权威 ”、“ 辅助服务器 ”和“ 区域 ”。

stateless / 无状态

针对服务器时，不包括基于客户请求的服务器端的数据库更新。针对文件的处理时，既不修改也不注意文件内容。对于 Web 服务器来说，

无状态的客户请求（网络负载平衡群集的成员能够处理）也就是那些给客户返回静态 Web 页面的请求。

static routing / 静态路由

指限制到固定路由表的路由，与动态更新的路由表相反。另请参见“ 动态路由 ”、“ 路由选择 ”和“ 路由表 ”。

status area / 状态区域

任务栏上任务栏按钮右边的区域。状态区域显示时间并还能够包含图标，通过这些图标可以快速访问程序，如声音控制和电源选项等。可能还会临时出现其它图标，它们提供了关于计算机上各项活动状态的信息。例

如：当一份文档被发送到打印机以后打印机图标就会出现，而当打印完成以后，打印机图标就会消失。

StickyKeys / 粘滞键

一种 Windows 内建的辅助功能特性，它能够使得在按下了如 SHIFT、CTRL 或 ALT 等修改键后它们能够保持按下状态，从而可以消除同时按下多个键的需要。该特性方便了那些不能在按下一个键的同时按住另一个键的用户使用修改键。

streaming media servers / 数据流媒体服务器

提供多媒体支持的软件（如 Microsoft Media Technologies 等），允许用户使用“ 高级数据流格式 ”通过内部网或 Internet 传递数据内容。

stripe set / 带区集

把数据存储在跨越不同驱动器的同一个分区内。带区集不提供容错功能；然而，带有奇偶校验的带区集就提供了容错功能。另请参见“ 容错 ”、“ 分区 ”、“ 带有奇偶校验的带区集 ”和“ 卷集 ”。

stripe set with parity / 带有奇偶校验的带区集

一种数据保护方法，在其中数据以大块的形式分带区存储在一个阵列内的所有磁盘上。奇偶校验信息提供了数据冗余。该方法提供了容错能力。另请参见“ 带区集 ”和“ 容错 ”。

striped volume / 带区卷

把数据分成多个带区并存储于两个或更多的物理磁盘之上的卷。连续的逻辑数据块分布于以循环的方式参与的磁盘之上，就象交织在一个多列内存系统中一样。每个数据“ 带区 ”由每个磁盘的一个数据块组成（包括所有的冗余数据）。

Structured Query Language (SQL) / 结构化查询语言 (SQL)

一种广泛接受的标准数据库子语言，用于查询、更新和管理关系数据库。

stub area / 存根区域

不公布个体外部网络的 OSPF 区域.在存根区域中到所有外部网络的路由选择都是通过一条默认路由（目的地址 0.0.0.0 且网络掩码为 0.0.0.0）来完成的。

subdomain / 子域

在名称空间树中直接位于另一个域名(父域)下的 DNS 域。例如：”eu.reskit.com” 是域 “reskit.com” 的子域。

subject / 主题

作用于某一对象上的实体。例如：当一个执行的线程打开某个文件的时候，该线程就是主题而该文件就是它的操作的对象。另请参见“ 对象 ”和“ 线程 ”。

subnet / 子网

IP 网络的一个子划分。每个子网都有唯一的子网 ID。

subnet mask / 子网掩码

由四个 0 到 255 之间的十进制整数表示的 32 位的值，之间用句号分隔（例如：255.255.0.0）。这个数

使得 TCP/IP 能够把 IP 地址的网络 ID 部分和主机 ID 部分区分开。

主机 ID 标识网络上的个体计算机。TCP/IP 主机使用子网掩码来确定目的主机是位于本地网络上还是远程网络上。

subnetting / 建立子网

把一个 TCP/IP 网络 ID 的地址空间划分成更小的网段的行为，每个更小的网段都有它们自己的子网的网络 ID。

switch / 交换机

一台计算机或其它联网的设备，用来控制路由选择和信令路径的操作。在群集中，交换机被用来把群集主机连接到路由器或其它传入的网络连接的源。请参见“ 路由选择 ”。

switched virtual circuit (SVC) / 交换虚电路 (SVC)

通过使用信令在 ATM 网络上的设备之间动态地建立的连接。

symmetric key / 对称密钥

对称加密算法在加密和解密时使用的单一的密钥。另请参见“ 批量加密 ”、“ 加密 ”“ 解密 ”和“ 会话密钥 ”。

symmetric key encryption / 对称密钥加密

一种要求在加密和解密时使用相同的密钥的加密算法。这种算法也常常被称为密钥加密。因为它的速度很快，当消息发送人需要对较大量的数据进行加密时通常使用对称加密而不是公钥加密。另请参见“ 公钥加密 ”。

Symmetric Multiprocessing (SMP) / 对称多重处理 (SMP)

一种计算机结构，其中多个处理器共享相同的内存，内存中包含操作系统的副本、当前使用的所有应用程序的副本以及数据的副本。因为操作系统把工作负载划分成任务并把它们分配给可用的处理器，SMP 缩减了事务处理时间。

Synchronization Manager / 同步管理

在 Windows 2000 中，用来确保客户计算机上的文件或目录与服务器上的匹配文件或目录包含相同的数据的工具。

Synchronized Accessible Media Interchange (SAMI) / 同步可访问媒体互换 (SAMI)

一种优化格式，用来在某个单一的文档中创建文字说明和声音描述。

synchronous processing / 同步处理

Windows 2000 中的默认组策略处理模式。在这一默认模式中在所有的组策略对象都被处理完成之前用户不能登录和在他们的计算机上开始工作。

Syspart

一个通过 Winnt32.exe 的可选参数执行的进程。用于到拥有不同的硬件的计算机的清洁安装。这种自动化的安装方法通过消除 Setup 程序的文件复制阶段，从而减少了安装时间。请参见“ 自动安装 ”。

Sysprep

一个为向目标计算机的复制而在源计算机上准备硬盘并随后运行一个第三方磁盘映像过程的工具当主计算机上的硬盘和目标计算机的硬盘相同时使用这一自动化的安装方法。请参见“ 自动安装 ”。

system access control list (SACL) / 系统访问控制列表（SACL）

代表某个对象的安全描述符的一部分，该部分指定对于每个用户或组将审核哪些事件。审核事件的范例是文件访问、登录尝试和系统关闭。另请参见“ 访问控制项（ACE）”、“ 自主访问控制列表（DACL）”、“ 对象 ”和“ 安全描述符 ”。

system files / 系统文件

Windows 用来加载、配置和运行操作系统的文件。一般说来，不能删除或移动系统文件。

system policy / 系统策略

指在网络管理中与注册表中的当前用户和本地计算机设置有关的组策略中那一部分。在 Windows 2000 中，系统策略有时被称作软件策略，它是一个“ Microsoft 管理控制台（MMC）”管理单元，即组策略提供的几个服务之一。为了达到向后兼容，Windows 2000 还包括了“ Windows NT 4.0 系统策略编辑器 ”，即Poledit.exe。即是说，管理员需要它来在 Windows NT 4.0 和 Windows 95 计算机上设置系统策略。另请参见“ Microsoft 管理控制台（MMC）”、“ 注册表 ”。

system state / 系统状态

在“ 备份 ”中，一组可以被备份和还原的与系统相关的数据。对于所有的 Windows 2000 操作系统来说，“ 系统状态 ”数据包括注册表、类注册数据库和系统启动文件。对于 Windows 2000 服务器操作系统来说，系统状态数据还包括“ 证书服务数据库 ”（如果服务器被用作证书服务器）。如果该服务器是域控制器，则系统状态数据还包括 Active Directory 和 Sysvol 目录。另请参见 “Active Directory”、“ 域控制器 ”和 “Sysvol”。

systemroot

Windows 2000 系统文件所在的路径和文件夹名称。一般情况下，它们位于 C:\Winnt 中，尽管当安装 Windows 2000 时可能会指定一个不同的驱动器或文件夹。值 %systemroot% 能够被用来替换包含有 Windows 2000 系统文件的文件夹的实际位置。要标识用户的 systemroot 文件夹，请单击 Start，再单击 Run，随后键入 %systemroot%。

Systems Management Server / 系统管理服务器

Windows BackOffice 产品套件的一部分。“ 系统管理服务器（SMS）”包括清单收集、部署和诊断工具。SMS

能够显著地自动化升级软件的任务，允许远程问题解决，提供资产管理信息，管理软件许可证并监视计算机和网络。

Sysvol

一个存储服务器的域公共文件的副本的共享目录，在域内的所有的域控制器之间复制。另请参见“ 域 ”、“ 域控制器 ”。

T

T1

一种以 1.544 Mbps 的速率传输数据的广域载波信号。

T3

一种以 44.736 Mbps 的速率和与 DS3 相同的格式传输数据的广域载波信号。

taskbar / 任务栏

包含有 Start 按钮的栏，默认时显示在桌面的底部。用户可以使用任务栏按钮来在用户运行的程序之间切换。任务栏可以隐藏，移动到桌面的边上或顶部，或以其它方式由用户自定义。另请参见“桌面”、“任务栏按钮”和“状态区域”。

taskbar button / 任务栏按钮

当应用程序运行时显示在任务栏上的按钮。另请参见“任务栏”。

TCP connection / TCP 连接

存在于两个使用 TCP 交换数据的进程之间的逻辑连接。

TCP/IP

请参见“传输控制协议 / Internet 协议”。

Telnet / 远程登录协议

一种 Internet 上广泛使用的终端仿真协议，用于登录到网络计算机上。Telnet 也指那些为来自远程位置的登录用户使用 Telnet 协议的应用程序。

terminal / 终端

一台由显示器和键盘组成的设备，用于与一台计算机通信。

text mode / 文本模式

Setup 中使用基于文本的界面的那部分。

thin client / 瘦客户

一台没有硬盘的网络计算机。

thread / 线程

进程中的一类运行程序指令的对象。使用多个线程允许一个进程内的并发操作，并使得一个进程可以在不同的处理器上同时运行它的程序的不同部分。一个线程有它自己的寄存器集、它自己的核心堆栈、一个线程环境块和在它的进程的地址空间内的一个用户堆栈。

throughput / 吞吐量

对于磁盘来说是磁盘系统的传输能力。

Time Service / 时间服务

在所有节点之间保持时间一致的服务器群集资源。

Time To Live (TTL) / 生存时间 (TTL)

基于 TCP/IP 的网络上传送的数据包中的定时器值，这个值告诉接收者在数据包或包中数据过期或被他丢弃

之前他应该持有或使用多长时间。对于 DNS 来说，区域内的资源记录中使用 TTL 值以确定当一条信息出现在该区域 DNS 服务器对查询响应的回答中时，作出请求的客户应该缓存和使用该信息多长时间，

ToggleKeys / 切换键

一项 Windows 的特性，当打开或关闭某一切换键（CAPS LOCK、NUM LOCK 或 SCROLL LOCK）时发出声响。

Token Ring / 令牌环

一种网络媒体类型，它连接一个封闭环中的客户并使用在客户之间传递的令牌来允许客户使用网络。另请参见“光纤分布式数据接口 (FDDI)”和“LocalTalk”。

topology / 拓扑

在 Windows 操作系统中，一组网络组件之间的关系。在 Active Directory 复制的上下文中，拓扑是指域控制器用来在它们之间复制信息的连接的集合。另请参见“域控制器”和“复制”。

transform / 转换

创建用来自定义安装行为的用户脚本，它直接修改安装脚本而不对应用程序重新包装。

transitive trust relationship / 可传递信任关系

天然地存在于一棵域目录树或目录林中的 Windows 2000 域之间，或在一个目录林的目录树之间，或目录林之间的信任关系。当一个域加入一个现存的目录林或域目录树时，将自动建立起可传递的信任关系。可传递的信任关系始终是双向的关系。另请参见“域目录树”和“目录林”。

Transmission Control Protocol/Internet Protocol (TCP/IP) / 传输控制协议 / Internet 协议 (TCP/IP)

广泛应用在 Internet 上的一组软件网络协议，能够提供相互连接的拥有多种硬件结构和操作系统的计算机组成的网络之间的通信。TCP/IP 包括计算机如何通信的标准及连接网络和路由通信的规范。

Transport Layer Security (TLS) / 传输层安全 (TLS)

一个用来提供在 Internet 或企业内部网上的安全 Web 通信的标准协议。它使得客户能够验证服务器的身份且服务器也能够验证客户的身份（可选）。它还通过加密通信提供了安全信道以实现机密性。

transport protocol / **传输协议**

定义如何把数据交给 Windows NT 和 Windows 2000 网络模型中的下一个接收层并相应地包装数据的协议。传输协议通过“网络驱动程序接口规范 (NDIS)”接口把数据传递给网络适配器驱动程序，并通过“传输驱动程序接口 (TDI)”把数据传递给重定向器。

Trivial File Transfer Protocol (TFTP) / 平凡文件传送协议 (TFTP)

IntelliMirror 服务器使用的一种协议，用来下载开始启动或安装过程时所需要的初始化文件。

trust relationship / 信任关系

域之间建立的逻辑关系，允许传递身份验证，在身份验证中信任域同意受信域的登录身份验证。在信任域中可以向在受信域中定义的用户帐号和全局组授予权限，尽管这些用户帐号或组在信任域的目录中并不存在。另请参见“身份验证”、“域”和“双向信任关系”。

trusted forest / 可信目录林

通过显式的或可传递的信任关系连接到另一个目录林的目录林。请参见“ 显式信任关系 ”、“ 目录林 ”和“ 可传递信任关系 ”。

TTL

请参见“ 生存时间 ”。

tunnel / 隧道

封装后的数据包通过中继网络传播时的经过的逻辑路径。

tunneling / 隧道

一种使用某种协议的互连网络基础结构来传送另一种协议的负载（帧或数据包）的方法。

tunneling protocol / 隧道协议

一种用来管理隧道和封装专用数据的通信标准。通过隧道传输的数据必须被加密成为 VPN 连接。Windows 2000 包括“ 点对点隧道协议 (PPTP) ”和“ 第二层隧道协议 (L2TP) ”。

two-way trust relationship / 双向信任关系

一种域之间的链接，在这种链接中每个域都信任另一个域中的用户帐号以使用它的资源。用户可以从任一域中的计算机上登录到包含他们帐户的域中。另请参见“ 信任关系 ”。

U

UDP

请参见“ 用户数据报协议 ”。

unallocated space / 未分配空间

未被分配给任何分区、逻辑驱动器或卷的可用的磁盘空间。在未分配空间上创建的对象的类型取决于磁盘类型（基本或动态）。对于基本磁盘来说，分区以外的未分配空间可以用来创建主或扩展分区。扩展分区内的可用空间能够被用来创建逻辑驱动器。对于动态磁盘来说，未分配空间能够被用来创建动态卷。不同于基本磁盘，不会选择确定的磁盘区域来创建卷。另请“ 参见基本磁盘 ”、“ 动态磁盘 ”、“ 扩展分区 ”、“ 逻辑驱动器 ”、“ 分区 ”、“ 主分区 ”和“ 卷 ”。

Unattended Setup / 无人值守安装

一种自动、无附加操作的安装 Windows 2000 的方法。在安装过程中，“ 无人值守安装 ”使用应答文件来向“ 安装程序 ”提供数据，而无须要求管理员交互式地提供应答。

UNC name / UNC 名称

网络上的资源的完整的 Windows 2000 名称。它遵循 \\servername\sharename 的语法，这里 servername 是服务器的名称而 sharename 是共享资源的名称。目录或文件的 UNC 名称也能够依照如下语法包括共享名下的目录路径：\\servername\sharename\directory\filename.UNC 又叫做“ 通用命名规则 ”。

unicast / 单播

一个地址，标识一个特定的、全局唯一的主机。

Unicode / 统一字符编码

一种固定宽度、16 位的字符编码标准，能够代表世界上大多数语言中的字母和字符。“ 统一字符编码 ”是由 U.S. 计算机公司协会开发的。

uninterruptible power supply (UPS) / 不间断电源供应系统 (UPS)

一种连接在计算机和电源之间的设备，用来确保电流不会中断。UPS 设备使用电池来使得计算机在停电后可以继续工作一段时间。UPS 设备通常提供对电源浪涌和电压过低的保护。

universal group / 通用组

一种只有在本机模式下才可用的 Windows 2000 组，在目录林中的任何地方都有效。通用组出现在全局编录中，但主要包含来自于目录林中的域的全局组。这是组的最简单的形式，且能够包含其它通用组、全局组和来自于目录林中任何地方的用户。另请参见“ 本地域组 ”、“ 目录林 ”、“ 全局编录 ”。

Universal Serial Bus (USB) / 通用串行总线 (USB)

一种双向、同步且可动态连接的串行接口，用于添加外围设备，如游戏控制器、串行口和并行口以及在单一总线上的输入设备等 。

UNIX

一种功能强大、多用户、多任务的操作系统，最初由 AT&T Bell Laboratories 在 1969 年为在小型机上使用而开发。因为它是用 C 语言写成的，所以人们认为 UNIX 比其他操作系统更具可移植性——即是说，更与计算机无关。UNIX 的新版本已经由 University of California at Berkeley 和 AT&T 开发出。

user account objects / 用户帐号对象

Windows NT Server 4.0 或 Windows 2000 Server 中用来标识某一特定用户的对象。

User Datagram Protocol (UDP) / 用户数据报协议 (UDP)

一个提供无连接数据报服务的 TCP 组件，既不能保证数据包的提交也不能保证它们的正确顺序。

user name / 用户名称

一个向 Windows 2000 标识用户帐号的唯一的名称。一个帐户的用户名称在它所在的域或工作组的组和用户的名称中必须是唯一的。

user password / 用户口令

存储在每个用户的帐户中的口令。每个用户通常都拥有一个唯一的用户口令，且每当登录或访问服务器时都必须输入该口令。

user profile / 用户配置文件

包含一位特定用户的配置信息的文件，如桌面设置、持续型网络连接和应用程序设置等。每个用户的选项都存储在一个用户配置文件中，每当有用户登录时，Windows NT 和 Windows 2000 可以使用该文件来配置桌面。

user rights / 用户权限

当用户登录时“ 密钥分发中心 (KDC) ”颁发给用户的凭据。当用户为服务请求会话票据时，他必须向 KDC 出示 TGT。因为 TGT 的有效期限通常是用户登录会话的整个生存期，它有时又被叫做用户票据。另请参见“ Kerberos 身份验证协议 ”、“ 密钥分发中心 ”和“ 会话票据 ”。

user ticket / 用户票据

请参见“ 票据授予票据 ”。

users / 用户

一个特殊的组，包含所有在服务器上拥有用户权限的用户。当一位 Macintosh 用户将权限分配给所有人时，这些权限会给予这个组的用户和来宾。另请参见“ everyone 的分类 ”和“ 来宾 ”。

Utility Manager / 工具管理器

Windows 2000 的一项功能，允许管理员复查应用程序和工具的状态并更加容易地自定义特性。

V

Virtual Circuit (VC) / 虚电路 (VC)

一条用来传输数据的点到点的连接。这就允许更好地控制各项呼叫属性，如带宽、潜伏期、延迟变化和顺序等。

virtual link / 虚拟链接

在骨干区域边界路由器和区域边界路由器之间的不与骨干相连的逻辑链接。

virtual memory / 虚拟内存

Windows 2000 用作内存的硬盘空间。因为虚拟内存的原因，从进程的角度看到的内存量可以比计算机上的实际的物理内存多。通过对不能放在物理内存中的数据分页并使它们在每时每刻都来回于物理内存和磁盘之间，操作系统以一种对应用程序透明的方式实现了功能。

virtual network / 虚拟网络

一种存在于 Novell NetWare 和与 NetWare 兼容的服务器和路由器中的逻辑网络，但是不与物理适配器相关联。虚拟网络在用户看来是分离的网络。在运行 Windows 2000 Server 的计算机上，程序公布自己在虚拟网络上的位置，而不是在物理网络上的位置。内部网络号标识了计算机内部的虚拟网络。另请参见“ 内部网络号 ”和“ 外部网络号 ”。

virtual private network (VPN) / 虚拟专用网络 (VPN)

专用网络的扩展，包括穿越共享或公共网络（如 Internet）的链接。

virtual private network connection / 虚拟专用网络链接

一个链接，在其中专用数据被封装和加密。

virtual private networking / 建立虚拟专用网络

配置和创建虚拟专用网络的行为。

virtual server / 虚拟服务器

在服务器群集中包含在某个资源组中一组资源，包括“ 网络名称 ”资源和 IP 地址资源。对于客户来说，虚拟服务器就象是一个运行 Windows NT Server 或 Windows 2000 Server 的系统。

voice input utilities / 声音输入工具

一种语音识别程序，允许残疾用户通过他们的声音而不是通过鼠标或键盘来控制计算机。

volume / 卷

物理磁盘的一部分，虽然它物理上分离，但是仍可以工作。在我的电脑和 Windows 资源管理器中，卷以本地磁盘的方式显示，如 C 或 D。

volume mount points / 卷装入点

Windows 2000 内部名称空间中新的系统对象，它以持久、健壮的方式表示存储卷。

volume set / 卷集

物理磁盘中的多个分区组合在一起，作为一个逻辑驱动器使用。另请参见“容错”和“带区集”。

VPN client / VPN 客户

初始化一个到 VPN 服务器的 VPN 连接的计算机。VPN 客户可以是一台获得了一条远程访问 VPN 连接的单独的计算机，或是一台获得了一条路由器到路由器的 VPN 连接的路由器。

VPN connection / VPN 连接

连接中用户数据得到加密时的连接部分。

VPN server / VPN 服务器

接受来自 VPN 客户的 VPN 连接的计算机。VPN 服务器能够提供远程访问 VPN 连接，和路由器到路由器的 VPN 连接。

W

Web server / Web 服务器

有能力开发基于 COM 的应用程序，和创建 Internet 和企业 Intranet 大型站点的服务器。

wide area network (WAN) / 广域网 (WAN)

连接物理上分离的计算机、打印机和其它设备的通信网络。WAN 允许任一连接设备与网络上的其他设备进行交互。另请参见“LAN”。

Windows 2000 MultiLanguage Version / Windows 2000 多语种版本

Windows 2000 的一种版本，通过允许每用户更改用户界面语言，扩展 Windows 2000 的母语支持。该版本还最小化了用户在跨网络部署时所需的语言版本的数目。

Windows 2000 Setup / Windows 2000 安装程序

安装 Windows 2000 的程序，又称为安装程序、Winnt32.exe 和 Winnt.exe。

Windows Installer / Windows 安装服务

一个 Windows 2000 组件，它通过要求每个应用程序都拥有自己的安装文件或脚本，标准化应用程序在多台计算机上的安装过程。

Windows Internet Name Service (WINS) / Windows Internet 命名服务 (WINS)

一种将IP 地址动态地映射到计算机名称（NetBIOS 名称）的软件服务。它允许用户通过名称访问资源，而无须使用难以辨认和记忆的 IP 地址。WINS 服务器支持运行 Windows NT 4.0 和更早版本的 Windows 操作系统的客户。另请参见“域名系统 (DNS)”。

Windows Management Instrumentation / Windows 管理规范

一种 Microsoft 技术，以连贯统一的方式表示存在于 Windows 管理环境中的物理和逻辑对象，调动桌面管理任务组 (DMTF) 基于 Web 的企业管理 (WBEM) 积极性。WMI 的设计将简化对良好集成的管理应用程序进行的开发工作，并允许供应商为企业环境提供高效、可扩展的管理解决方案。

Windows 套接字 (Winsock)

一种工业标准的应用程序编程接口 (API)，用于 Microsoft Windows 操作系统，以提供双向、可靠、有序而且无法复制的数据流。

Windows-based terminal / 基于 Windows 的终端

使用 Windows 操作系统的终端。

WinInstall LE

Windows 2000 Server 附带的重新打包工具。

WINS

请参见“Windows Internet 名称服务”。

WINS database / WINS 数据库

用于注册和将计算机名称解析为基于 Windows 的网络 IP 地址的数据库。该数据库的内容以固定的时间间隔在网络中被复制。另请参见“发送伙伴”、“接收伙伴”和“复制”。

WINS proxy / WINS 代理

用于侦听名称查询广播，并对非本地子网的名称进行响应的计算机。代理通过与名称服务器通信，解析名称，并将它们在缓存中保存一段特定时间。另请参见“Windows Internet 名称服务 (WINS)”。

X

X.509 version 3 certificate / X.509 版本 3 证书

ITU-T 推荐标准中关于语法和格式的 X.509 版本 3。Windows 2000 中基于证书的进程使用它作为标准的证书格式。一份 X.509 证书包含：领取证书的个人或实体的公钥和信息、证书信息，以及颁发证书的证书颁发机构 (CA) 的可选信息。另请参见“证书”和“公钥”。

Z

ZAP (.zap) file / ZAP (.zap) 文件

零管理 Windows 应用程序包文件。一个文本文件（类似于 .ini 文件），描述如何安装应用程序（使用哪些命令行）、应用程序属性（名称、版本和语言）以及该应用程序应该自动安装哪些入口点（为文件扩展名、CLSID 和 ProgID）等信息。.zap 文件通常与相应的安装程序存储在网络中的相同位置。

zone / 区域

在 DNS 数据库中，区域是 DNS 目录树中的毗邻部分。DNS 服务器将它作为单独的孤立实体进行管理。区域包含该区域内所有名称的资源记录。在 Macintosh 环境中指一种逻辑分组，该分组可以简化网络资源浏览（例如服务器和打印机）。类似于 Windows 2000 Server 网络中域的概念。另请参见“域”、“域名系统 (DNS)”和“DNS 服务器”。

zone transfer / 区域复制

DNS 服务器通过该进程进行交互，以维护权威名称数据，并使之同步。当 DNS 服务器被配置为某个区域的辅助服务器时，它将定时地查询该区域中，被配置为它的源的主 DNS 服务器。如果主服务器保存的区域版本与辅助服务器不同，那么辅助服务器将从它的主 DNS 服务器中提取区域数据进行更新。另请参见“完全区域复制 (AXFR)”、“增量区域复制 (IXFR)”、“辅助服务器”和“区域”。