Mastering Active Directory for Windows Server 2003 Third Edition

Windows Server 2003 活动目录从入门到精通

（第三版）

〔美〕 Robert R. King 著

薛 菲 王曼珠 等译

薛荣华 审校

- 理解活动目录的内在机制
- 设计并运行活动目录以满足商业需求
- 逐步指导读者掌握关键管理任务

SYBEX

電子工業出版社
Publishing House of Electronics Industry
http://www.phei.com.cn

内 容 提 要

活动目录是Microsoft网络中的一项重要服务和网络管理的一个重要工具，是当今计算机网络的主流技术。本书从目录的基本概念开始，引导读者逐步理解活动目录的原理和操作，并掌握活动目录的设计和实施以适合各种规模环境的需要。本书已经完整更新到Windows Server 2003活动目录的新特性，是一本关于活动目录技术全面、深入的参考书。

本书适合网络管理员、计算机高级用户和大专院校计算机专业师生阅读使用。

版权贸易合同登记号：01-2003-0348

图书在版编目（CIP）数据

Windows Server 2003活动目录从入门到精通（第三版）/（美）金（King, R. R.）著；薛菲等译.—北京：电子工业出版社，2003.7

书名原文：Mastering Active Directory for Windows Server 2003 Third Edition

ISBN 7-5053-8768-5

Ⅰ. W… Ⅱ. ①金… ②薛… Ⅲ. 服务器－操作系统（软件），Windows Server 2003－目录 Ⅳ. TP316.86

中国版本图书馆CIP数据核字（2003）第041694号

责任编辑：郝黎明 张 洋

印 刷：北京天竺颖华印刷厂

出版发行：电子工业出版社 http://www.phei.com.cn

北京市海淀区万寿路173信箱 邮编：100036

北京市海淀区翠微东里甲2号 邮编：100036

经 销：各地新华书店

开 本：787×1092 1/16 印张：24.625 字数：630千字

版 次：2003年7月第1版 2003年7月第1次印刷

定 价：42.00元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换，若书店售缺，请与本社发行部联系。联系电话：（010）68279077

献　词

献给笔者的妻子和挚友——Susan

致　谢

笔者虽然出版过几本书，但不敢称自己是出版界的“老手”。笔者仍然对许多人在一起工作生产出高质量的资料感到惊讶。有许多人帮助把这本书送到读者的手里——并且每个人对这一过程都很重要。

首先，笔者要深深地感谢Bob Abuhoff对本书第三部分的贡献和Marcin Policht对第11、12章和第13章的审阅。没有他们的帮助，笔者无法按时完成这个项目。

感谢笔者的家人。每次笔者开始一项Sybex项目，笔者答应他们将按正常的时间表工作，但每次结束工作都要晚几小时。这本书没有他们的爱心和支持就不可能完成。

感谢James Gibson，是他给了没有经验的笔者在这个行业第一份工作的机会。

还要感谢Sybex的工作人员，他们是具有支持和理解力的人们。选题编辑Ellen Dendy和开发编辑Tom Cirtin按照版本的变化指导过笔者。编辑Anamary Ehlen是富有洞察力的，确实帮助过笔者确保本书保持一致的风格。生产编辑Lori Newman和Publication Services的电子出版专家Scott Benoit使本书的最终产品看上去更加靓丽。最后，衷心感谢笔者的技术编辑James Kelly确保笔者摆脱困境！对所有帮助本书出版的人们，让笔者再道一声：“谢谢！”

译 者 序

活动目录（Active Directory，AD）是Microsoft网络中的一项重要服务和网络管理的一个重要工具，是当今计算机网络的主流技术。本书从目录的基本概念开始，引导读者逐步理解活动目录的原理和操作，并掌握活动目录的设计和实施以适合各种规模环境的需要。

本书共分三大部分。第一部分是基础知识，包含许多概念性信息，介绍目录服务及其益处，概述X.500建议和两个用来访问AD数据库中存储信息的协议——DAP和LDAP。第二部分是Microsoft活动目录服务的基本内容，包括网络支持服务、设计活动目录环境、创建安全的环境、实现自己的设计、实现组策略、修改活动目录方案以及理解和控制AD站点及复制。第三部分是高级活动目录管理。包括活动目录网络通信量、活动目录的备份与恢复、活动目录设计、迁移到活动目录以及活动目录与Novell目录服务的集成。本书已经完整更新到Windows Server 2003活动目录的新特性，是一本关于活动目录技术全面、深入的参考书。

本书由薛菲（第1章～第10章）、王曼珠（第11章～第18章）翻译，由薛荣华审校并统稿。参加本书译录校工作并给予大力协助的还有闫慧娟、曹汉征、许秀英、王泰东、矫克民、王景中、徐小青、姚栋、徐凤麟、薛晏、刘晓玉、刘东顺、沈兰英、赵继红、李可、郭淼、王建成等同志。译者谨向所有为本书的出版提供帮助的同志表示由衷的谢意。由于译者水平有限，译文中难免有不妥之处，欢迎读者批评指正。

欢迎与我们联系

为了方便与我们联系，我们已开通了网站（www.medias.com.cn）。您可以在本网站上了解我们的新书介绍，并可通过读者留言簿直接与我们沟通，欢迎您向我们提出您的想法和建议。也可以通过电话与我们联系，电话号码（010）68252397。

简　介

虽然笔者曾写过几本关于Microsoft产品的书，但笔者不想隐瞒笔者一开始是一位Novell信徒的事实（一段时间笔者曾是Novell的雇员）。当Microsoft首次发布Windows NT时，笔者奇怪为何那么多人购买“新技术”（NT）。他们的“新技术”——或至少是它的网络部分——一个已经开发了10年的IBM产品，名为LanManager（通过任何NT计算机搜索“Lanman”一词将证明这一点）。所以，Microsoft发布了一个基于10年网络哲学的产品，并且默认情况下使用了一个不可路由的通信协议。对笔者来说，它似乎并不“新颖”！

Windows 2000/Windows Server 2003将Microsoft网络从早期版本的过时的、限于以域为基础的体系结构转移到真正基于目录服务的体系结构，这是当前复杂网络所需要的。Microsoft通过增加活动目录（Active Directory，AD）提供这个服务，它是一个开放的、基于标准的、兼容X.500以及LDAP可访问的网络目录。（不必担心，本书将讨论X.500和LDAP等似乎是无止境的首字母缩略词的含义。）

第一个商业上可行的、基于目录服务的操作系统是Novell带有NetWare Directory Services（NDS）的NetWare 4。在它发布时，笔者在美国明尼苏达州明尼亚波利斯一家公司任高级技术指导。为了在竞争中领先一步，公司派笔者去参加该软件测试版的预备班。两个星期的NDS强化培训后，笔者回家并开始重新评估笔者的职业选择。笔者感到，似乎以前关于网络所掌握的一切已经过时，笔者必须掌握称为“目录服务（directory service）”的新范例。必须承认，当第一次看到Novell的目录服务时，笔者没有掌握它，没有想过笔者会掌握它并且不敢肯定想掌握它。笔者感到NetWare的早期版本是安全的，不理解为什么有人想给他们的网络添加目录服务的复杂性。然而，在长期运行中，目录服务的好处远远超过痛苦的学习曲线。随着活动目录作为Windows 2000 Server产品的一部分发布，Microsoft最终将这些好处提供给它的客户群。（笔者希望本书能减少掌握该技术所涉及的痛苦！）

AD在当今变化的计算机世界中提供动力和灵活性，但提供是有代价的。大部分代价是为了充分理解和利用Microsoft Windows 2000/Windows Server 2003和活动目录服务（Active Directory Services）的潜能，管理员需要攀登陡峭的学习曲线。然而，使用活动目录自有它的好处：

一个更加稳定的操作系统　极少见到以前在Microsoft环境中出现的“蓝屏”。可以和每周（或更多）为保持NT服务器运行所需的重启说再见。

组策略　控制最终用户环境——他们能看见什么、能改变什么和能做些什么——作为越来越复杂的操作系统是重要的。

软件发布　统计表明，网络专业人士在安装和维护最终用户应用程序方面要比其他方面的工作花更多的时间。使这些工作自动化将允许我们（最终）利用多年来累积的一些休假时间！

本书有助于避免被Microsoft Windows 2000/Windows Server 2003和Active Directory的惊奇所捕获。对读者来说，网络目录可能是联网中的一个新范例，尽量记住它大部分基础、网络技术——无论Windows 2000/Windows Server 2003、AD或别的什么——只是从一处到另一处移动一点点。收集的所有联网知识仍然有效，只是可用的选项再多几个。

本书的内容

在计划本书的内容时，尽力最佳展示Microsoft网络的一个新范例——网络目录的概念。有人建议笔者只写与活动目录服务有关的内容，其他方面听之任之，但笔者还是想让读者在了解AD的同时对这种技术有一个总体的认识。笔者决定将本书分为三个部分以实现这个目标。下面是每个部分的内容。

第一部分：网络目录基础

无论Microsoft如何宣传，网络目录实际上已经出现了相当一段时间。理解早期的实现（它们的优点和缺点）有助于理解AD的工作原理——也许还有助于认识它的某些弱点。第一部分内容很短，但它包含许多概念性信息，可以真正帮助读者将AD结合到自己的工作环境中。第一部分包括四章。

第1章：网络目录服务及其益处 这一章给出了什么是目录以及什么是活动目录的基本概述，并且与过去使用的目录技术做了对比。

第2章：网络目录剖析 本章通过查看现有技术的实例学习什么是目录，从基本的书面目录开始，逐渐进入当前网络中使用的目录。

第3章：适应X.500标准的目录 这一章概述了X.500建议，它用来创建活动目录数据库的结构。我们还讨论从头创建一个目录服务数据库的过程——能确实有助于理解生成活动目录的智力练习。

第4章：目录的访问 第4章解释DAP和LDAP，两个用来访问AD数据库中存储信息的协议。

第二部分：Microsoft活动目录服务

一旦有了目录技术的坚实基础，就可以用一种审视的眼光看待AD，试图找出它的优点和缺点。利用这个信息，就可以更好地在自己的环境中应用该技术。第二部分有九章。

第5章：没有AD的Microsoft网络 要充分了解Windows 2000/Windows Server 2003，尤其是理解活动目录，重要的是理解NT的早期版本。如果读者是一位NT专家，可把这一章作为复习。如果读者是NT领域的新手，这一章是本书后面遇到的某些课题的准备。

第6章：活动目录的益处 就像NT最初设计出来是为了克服以服务器为中心的环境的弱点那样，带AD的Windows 2000/Windows Server 2003的设计是为了克服基于域的环境所存在的弱点。本章讨论AD如何适合于Windows 2000/Windows Server 2003的总体哲学。

第7章：网络支持服务 虽然Microsoft的Windows 2000/Windows Server 2003可以利用许多不同的通信协议，AD却依赖于TCP/IP。在安装和配置AD环境之前，必须先对TCP/IP工具和技术有一个全面的了解。

第8章：设计活动目录环境　本章介绍设计一个稳定的AD结构的理论，该结构不对网络的任何单独部件施加不适当的压力。

第9章：实现自己的设计　本章介绍AD安装和建立AD结构的机制。

第10章：创建安全的环境　如果AD数据库希望在网络中得到任何实际应用，它包含的信息必须是安全的。本章将查看Windows 2000/Windows Server 2003中可用的各种安全选项。

第11章：实现组策略　组策略用于一次性地为整个用户组或计算机组定义用户或计算机设置。因此，它们对基于Windows 2000/Windows Server 2003网络的管理员是一个非常重要的概念。本章讨论组策略的概念并介绍实现这些概念的过程。

第12章：修改活动目录方案　AD数据库包含对象类和属性，对象类定义网络资源的类型，而属性定义这些类的参数。默认的类清单和属性在某些环境中可能不够。本章讨论扩展AD数据库设计，包括自定义对象类和属性的过程。

第13章：理解和控制AD站点及复制　对于任何网络操作系统，不论设计的结构如何符合逻辑，也不论制定的图形化界面如何直观，一旦工作完成了，所有的数据都要通过“管道”来传递。本章从可用带宽和通信成本的观点讨论设计问题。

第三部分：高级活动目录管理

至今为止，已经在第一部分中从历史的角度掌握了建立活动目录的技术历史。在第二部分中查看了活动目录环境的基本结构——设计策略、通信量考虑和在大多数AD环境中发现的外围组件。第三部分将深入考察活动目录实现的特殊部分。

第14章：活动目录网络通信量　本章讨论网络上产生通信量的设备和服务。虽然没有人能描述通过网络连线的每一个位，但我们将查看涉及活动目录DNS、WINS、DHCP和AD复制等服务。

第15章：活动目录的备份与恢复　每个人都知道好的备份对工作安全性是极为重要的——公司里的每个人都能描述基本的服务器备份。许多人并不理解备份一个复杂的数据库（如活动目录）的复杂程度。我们将查看涉及活动目录备份和恢复中的理论和工具。

第16章：活动目录设计　设计分层系统的方法多种多样。我们将查看几个影响最终AD设计的网络和商业细节。还提供几个能起基础作用的示例设计。

第17章：迁移到活动目录　很少人有从头开始的奢华——我们继承一个网络，然后想要升级它以适应认识到的需要。本章将讨论想升级现有网络到Windows 2000和活动目录时可用的选项。

第18章：活动目录与Novell目录服务集成　Novell仍然把持着商业网络市场的一个重要部分。最近的一些调查甚至表明，NetWare的市场份额可能在增加。甚至在所有新服务器都是基于Microsoft的公司里，许多仍然继续支持遗留的NetWare服务器。在读者的职业生涯中有时会面临一个混合的环境。本章将讨论有助于支持两种平台：AD和NDS的工具和技术。

本书的读者对象

本书针对的读者是具有一定经验并希望了解Microsoft活动目录服务的网络管理员。本书假定读者对网络已具备一般的基础知识，但是还不（或很少）了解基于目录的技术。尽管Microsoft所做的活动目录是业界转移的一个大方向，但如果运行的是Microsoft的系统，就需要赶快加速到AD；如果运行的是一个非Microsoft的系统（或更老版本的Windows NT），可以打赌，不久读者就需要理解Microsoft是如何看待网络目录的。

在笔者做技术指导的10年中，发现有两类学生——一些只想知道“如何”，而另一些还想知道“为什么”。笔者认为，本书将满足两类计算机专业人员。我们当然要钻研理论——讨论网络目录的历史、管理目录的哲学和影响AD最终设计的与环境有关的各个方面。我们还讨论并描述了许多更加常见的管理任务，这些将是日常需要执行的任务。理论和实际的结合应该为实现和维护网络环境中活动目录结构的任务做好准备。

笔者相信，最后会出现这样一种情况：如果人们现在已经联网并且将来仍然在网络环境中工作，就必须在将来某一天掌握网络目录的概念。本书的目的就是给人们以理解和实现Microsoft的这项技术所需的信息。

小结

Microsoft Windows 2000/Windows Server 2003是当今网络中最热门的技术。要有效地使用它，也许不得不重新思考如何特性化网络资源和服务。建立网络然后再考虑环境的日子已经过去！借助今天的技术，每个网络将不得不围绕一个“总体商业解决方案”进行设计——提供资源和必要的服务而无须公司过度繁重的预算、人员或基础设施。

最后一句忠告：享受新技术。新技术可能是激动人心的、富有挑战的和十分有趣的。如果花时间抱怨新技术而不是去欣赏它，也许不如去休假！

与笔者编写的所有书一样，如果读者对书中的内容有问题或意见，请给笔者发邮件：bking@royal-tech.com。笔者始终盼望收到反馈。

目　录

第三部分 高级活动目录管理

第一部分

网络目录基础

本部分将学习：

- 评价网络目录服务及其益处
- 理解目录系统的重要特性
- 设计普通目录
- 访问目录

第1章 网络目录服务及其益处

计算机业，特别是网络领域，产生的缩略语、术语、短语和时髦用语比世上其他任何领域都要多。近来最热门的莫过于短语网络目录（network directories）。目录一词没有什么新鲜的，从20世纪60年代这个词就以各种形式出现了。但是现在，这个词已经随着被期盼已久的Microsoft公司Windows 2000 Server和Windows Server 2003产品线中Active Directory Services（活动目录服务，ADS）的发布而进入了主流。为了从这项技术中获得最大收益，人们必须透彻地理解目录是什么，不是什么，以及怎样用目录来简化网络的管理。这就是编写本书的目的——为读者提供充足的信息以实现、管理和利用Microsoft公司的Active Directory Services（ADS）所提供的服务（尽管目录只是Windows 2000和Windows Server 2003环境的又一项功能，但是它已经达到了“摇滚明星”的地位——有了缩略语。Microsoft公司的目录服务通常被称做Active Directory或者AD。笔者在本书中也将贯穿使用这个术语）。

基于PC的网络已经成为商业世界中的重要组成部分。它们起初是作为简单的解决方案来共享一些物理资源，如硬盘空间、打印机，等等。然而，随着时间的推移，网络已经变得十分复杂，常常跨越多个站点，将成千上万的用户与大量资源连接在一起。今天，网络几乎控制着从工资单资料到电子邮件通信，从打印机到传真服务等各项工作。随着网络提供的服务的增加，网络管理的需求也大大增加。简化网络的使用和管理成了目录服务的真正目标。

本书的第1章与其说是技术内容，不如说是为书中的第一部分设定恰当的情境。目录能够简化（有时甚至可以去除）一些最普通的IT管理任务。本章中会谈到这样几个任务，想想我们在“传统”网络中会怎样操作，然后想像一下目录如何使其更便于处理。本书最基本的目的是展示目录这一令人兴奋的技术，并且让读者开始为之兴奋起来！当然，要达到兴奋状态，必须牢固掌握目录的概念。本章的第一部分将解释什么是目录，使用目录有什么益处，并且介绍当今市场上大多网络目录采用的基本结构。

笔者在这个行业工作的时间相当长了，知道IT部门的典型工作环境是怎样的。首先，IT工作者通常被认为是“夜行者”——在其他人都结束了一天的工作回家后（更糟糕的是在周末或节假日），他们才能做自己最重要的工作（服务器维护，数据备份，升级，等等）。其次，IT工作者被认为应该是工作狂。为什么他们有假期却似乎从来都不能利用？数不清有多少次听到IT工作者由于无法休假在年末失去了休假的机会——因为总是会发生一些事情使他们不可能离开一个星期左右的时间。最后，他们被认为应该知道任何事情（虽然他们也喜欢这样的形象，但它有时确实给他们造成了麻烦）。去年参加了多少次培训班？有多少次是自愿参加的？如果这两个数字相等（或接近），那么这家公司是一家不错的公司！很多时候，IT工作者没有时间参加培训，这又造成更频繁的加班，更多头疼，和更少有机会使用假期。

多数管理员工作量太大而工资太低。多数IT部门人数不足且预算太低。这使得IT专业人员不能与家人在一起，不能参加培训课程（这又使问题更严重），很少有时间放松——难怪他们当中很多人在面对中年危机的时候改变了职业！

活动目录（Active Directory）被正确安装和配置后，通常可以减少网络维护的管理量。某些任务彻底被消除，很多多余的任务被简化到仅仅一步，多数管理过程更容易完成。起码读者的工作日会更有效率——使读者能接受更多职责，能利用读者的假期，或许也能参加一些读者向往已久的培训课程和行业论坛。（是的，这是积极的想法。很可能，公司会认为所需的IT员工数减少，读者会因为裁减IT员工而失去工作。也不全都是如此糟糕，因为较少员工数量往往带来更高的工资。这是双赢的情况！）

为活动目录而兴奋吧！虽然它要求读者掌握一个新的范例（将此理解为要攀登的学习曲线吧），它毕竟给读者更高效率地工作提供了机会！IT部门常常会因此为系统引进新的（令人兴奋的）技术。如果读者和笔者一样，就会把利用最新最棒的技术视为工作中的又一可喜的事情。

本章包括以下内容：

- 什么是目录服务
- 为什么使用目录服务
- 网络目录出现以前
- 传统网络与网络目录的对比
- 活动目录的益处
- 活动目录的结构
- 活动目录的特性集

什么是目录服务

在任何商业层面的联网环境中，都存在某种形式的账户信息数据库。在Windows NT中，该数据库称为Security Accounts Manager（SAM，安全账户管理器）数据库，而在Novell NetWare的早期版本中，叫做bindery。无论读者面对何种网络操作系统，总会有一个地方用来存储有效用户的信息，如名字、口令或是一些保密信息。

在多数操作系统中，账户数据库都是以服务器或资源为中心的。也就是说，数据库仅仅存储那些有权访问位于数据库所存储的设备控制范围之内的资源（文件、打印机、应用程序等）的用户信息。Novell的bindery是一个很好的例子：它为有权访问特定服务器（bindery文件所在的服务器）的用户存储账户信息。当该类型系统用于较小的环境时，会随网络的增大而崩溃。试想，每台服务器有自己的账户数据库，笔者有100台服务器，那么笔者就有100个账户数据库需要管理。

目录服务是一个存储诸如用户账户等资源信息的网络范围的数据库。在基于目录的环境中，笔者为每个用户创建一个单独的用户账户，用于管理用户网络（有时是桌上电脑）环境的所有方面。换言之，目录服务为基于网络的实体信息存储提供一个场所，这些实体包括应用程序、文件、打印机或使用者。在这样网络范围中的数据库就为各种资源的命名、描述、定位、访问、管理和保密信息提供了一个一致的办法。

目录也是控制和管理网络操作系统的中心点。它是正确识别和认证资源身份的中央权威，同时协调各分散资源间的关系，允许它们共同工作。目录服务必须与底层的操作系统紧密相联，以确保网络信息的完整性和保密性。

在基于Microsoft的网络中，Active Directory Service在决定公司管理网络基础设施、执行系统管理和控制用户环境的能力高下方面扮演了关键角色。

为什么使用目录服务

当笔者初次涉足网络行业时，是在当时的中等规模的环境中工作——有4台服务器和大约200位用户。因特网还是很遥远的事情，电子邮件也很不普及（甚至大多数人并不知道电子邮件为何物），还没有出现“传真服务器”或任何专门服务器。FedEx用于两地间的文件传递（没有人想过为中等规模的企业投资一种广域连接——那简直太昂贵了）。

而今天，一个中等规模的环境可以包括50台或更多数量的服务器，支持不说成千也有几百位用户，在专用服务器上提供大量专门服务。广域连接如今十分普遍，对带宽的需求是天文数字！更不用说拨入服务、虚拟专网（VPN）和其他终端用户需要的“新”业务。在这样复杂的网络中，对基于网络的多资源的管理工作可谓重之又重。

目录可以通过以下方面帮助管理员管理当今的复杂环境：

- 简化管理。作为管理的单点（并提供一个一致的管理工具集），目录可以使得与复杂网络相关的管理任务变得简单。
- 提供更强的安全性。上面提到，访问和认证是通过单一服务来控制的，管理员和用户只需要知道一套工具，所以对这套工具理解更透彻。目录提供单一登录工具，因此，通常能提供更为安全的认证程序（由于所有登录都受中心服务管理，因此，该服务非常安全）。
- 提高互操作性。当今，多数的商用目录服务（包括AD）都是基于一系列行业标准——X.500和LDAP命名的一些标准（笔者将在后面谈到）。采用基于标准的解决方案更易于在混合环境中共享资源，更妙的是，能够与商业伙伴共享资源却避免在网络上打开过多的大门。

目录可视为管理工具，也可视为用户工具。从管理的角度来看，使用资源信息的集中控制并保持一致的界面会大大降低管理成本。从用户的角度来看，认证的中心服务更易于网络资源的访问。用户不得不记忆（更糟的是写在贴纸上）多个登录名和口令的日子一去不返了！

网络目录出现以前

要想理解基于目录的解决方案的强大威力和欣赏它所带来的方便，就必须要了解它所替代的技术。在目录出现之前，大多数网络操作系统（NOS）都是“基于服务器”的系统。也就是说，大多数账户管理工作都要一台一台服务器地逐个进行。采用旧式NOS软件，每台服务器都维护一个可访问其资源的用户清单（即账户数据库）和用户许可清单（访问控制列表，Access Control List或ACL）。如果一个系统有两台服务器，则每台服务器都有一个独立的账户数据库，如图1.1所示。

图1.1 基于服务器的NOS

可以看出，图1.1中的每台服务器都要维护一份自己的授权用户清单，并且管理各自的资源。这种系统虽然很简单，易于理解，但是一旦系统增长到一定程度，就会变得很难处理。假设要管理250台服务器上的10 000个用户，光用户和资源清单就会立刻吓倒读者！为了避开这种缺陷，一些NOS软件，如Microsoft NT 4，被配置成一小组服务器共享用户清单（称为中央账户数据库），以达到确保安全和认证的目的，如图1.2所示。这种中央账户数据库为系统管理员提供了部分网络的集中管理点，称为域（domain）。然而，当这种系统增长到一定程度时，它也会变得笨重不堪。

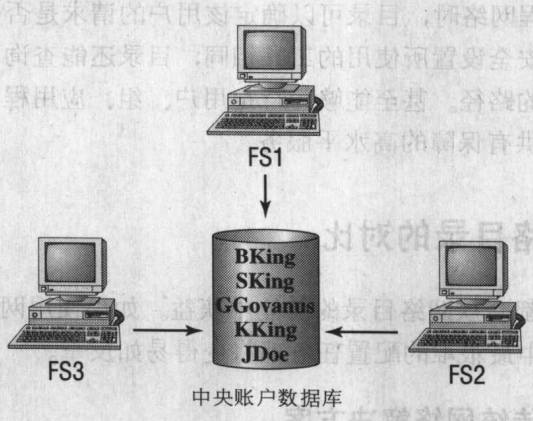

图1.2 NT 4安全账户数据库

基于服务器到基于域的网络转换，完成了创建用单一数据库管理所有用户和资源环境的第一步。在域中，所有用户信息都存储在同一个地方，用同一套工具进行管理，并且用户可以通过同一个账户访问网络（不用记住多个账户名和口令）。网络目录在此基础上又前进了一步：在整个网络中使用一个数据库存储所有用户和资源的信息。

说明： 书中“用户和资源”是指目录数据库中的记录，因为在传统的管理员看来，就是用户访问资源。在基于目录的环境中，用户只不过是另一种资源而已。这种思想上的转变对于理解基于目录的网络的威力十分重要。随着对目录概念的逐步了解，读者也会明白其中的不同。