Mastering Active Directory

Active Directory
从入门到精通

〔美〕Robert R. King 著
马树奇 等译

揭开Windows 2000关键技术Active Directory服务的神秘面纱

了解Active Directory如何改变用户管理网络的方式

理解Active Directory原理、实现和管理

资料源于即将面世的Windows 2000系统

NETWORK PRESS SYBEX

PHEI

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

Mastering Active Directory

Active Directory
从入门到精通

〔美〕Robert R. King 著

马树奇 等译

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 提 要

本书全面地介绍了即将面市的Windows 2000 Server及Active Directory技术。本书由浅入深地从基本概念开始，介绍了系统中各个重要的核心环节。

全书分为三大部分，第一部分讲述网络目录的背景和历史，介绍了网络技术的总体发展情况。第二部分介绍了即将面市的网络目录代表作：微软公司的Active Directory Servers技术。第三部分讲述Active Directory Services对未来的技术发展和产品可能造成的影响。

本书不是简单的大量屏幕图像组成的使用手册，也不完全是纯理论讨论，而是把两者有机地结合起来，其内容丰富实用，不仅适用于网络系统管理员、网络设计人员，也适用于高校学生、教师。

图书在版编目（CIP）数据

Active Directory从入门到精通/（美）金（King, R. R.）著；马树奇等译. —北京：电子工业出版社，1999.11
书名原文：Mastering Active Directory
ISBN 7-5053-5637-2

Ⅰ. A… Ⅱ. ①金… ②马… Ⅲ. 计算机网络－操作系统（软件），ActiveDirectory Ⅳ. TP393

中国版本图书馆CIP数据核字（1999）第65733号

书　　名：Active Directory从入门到精通
著 作 者：〔美〕Robert R. King
译　　者：马树奇　等
责任编辑：春丽
印 刷 者：北京天竺颖华印刷厂
装 订 者：三河金马印装有限公司
出版发行：电子工业出版社　URL: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：18.375　字数：470千字
版　　次：1999年11月第1版　1999年11月第1次印刷
书　　号：ISBN 7-5053-5637-2
　　TP·2891
定　　价：31.00元

版权贸易合同登记号　图字：01-1999-2981

献给我的妻子和最好的朋友——Susan

致　　谢

我对出版工作还感到相当新鲜。我曾经与Sybex公司在其它一些项目上有过合作（项目名称是Sybex Exam Notes——Sybex考试注释系列），至今还对他们致力于完成各种高质量产品的忘我工作记忆犹新。有许许多多的人为使读者能够看到这本书而努力工作——他们都为完成这个项目做出了不可缺少的贡献。

首先要感谢我的家人。每当我开始从事一项新的Sybex项目开发时，都会向他们许诺说“我会制定一份正常的工作计划”，而实际上却又常常工作到凌晨。没有他们的爱与支持，就没有这本书的出版。

我还要感谢Sybex的工作人员。他们是我所遇到的人中最具有支持和理解力的人们。本书的开发编辑Maureen Adams和项目编辑Jeremy Crawford都能够在我无法及时完成某些工作时给予了充分的理解。编辑Nancy Conner以她那行家的眼光使本书始终能够保持一致的风格。项目组负责人Shannon Murphy和电子出版专家Robin Kibby使这本书最终成为靓丽的成品。最后，我的技术编辑Don Fuller使我一次次地从困境中解脱出来，衷心感谢他的帮助！对所有这些人们和所有对本书的出版做出贡献的人们，我在此衷心地道一声“谢谢！”。

译 者 序

IT行业的发展日新月异，从事IT行业的人都有同感。谁能够在技术的发展过程中把握先机，谁就更有机会赢得市场的主动权。IT从业人员需要不断更新自己的技术以适应社会发展的要求，而如果能够领先一步掌握即将到来的主流网络技术，则是多数人的愿望。

本书非常适时地在微软公司下一代主流网络操作系统产品面市之前，以测试版为基础，系统地介绍了这种即将对技术发展产生深远影响的新产品涉及到的一些基本技术和产品特点，对于具有一定网络应用基础的网络从业人员率先掌握二十一世纪的主流网络技术十分有利。无论是网络系统管理员、网络设计人员还是工程人员，甚至高校学生、教师，掌握IT最新、最重要的主流技术都是十分必要的。本书不是简单的、大量屏幕图像组成的使用手册，也不是抽象、艰深的纯理论探讨，而是把两者有机地结合起来，既深入浅出地介绍了ADS技术的基本原理，又根据Windows 2000测试版把系统中最重要的设置步骤讲述清楚，同时篇幅又不是很长，实在是一本优秀的著作。

译 者

1999年6月

前　言

在过去几年中，微软公司的Windows NT 4已经对网络市场造成了极大的冲击，成为最热门的“新”技术。由于Windows NT 4系统在长达10年的时间里始终是一种以域为基础的模型，因此它获得了这样的成绩总让我感到不可思议。换句话说，微软公司所谓的最新技术实际上并不那么新颖。但这种情况正在改变，这就是NT系统的下一代版本——Windows 2000 Server。

Windows 2000 Server把微软网络技术从以前版本中过时的（也是受局限的）以域为基础的体系结构带入了真正基于目录服务的结构，这正是当前网络日益复杂化的发展需要。微软公司通过引入Active Directory Services（主动目录服务，ADS）提供这种技术服务，它是一种开放的、以现有标准为基础的、兼容X.500标准并且可以访问LDAP的网络目录（别担心，我们会在本书后面内容中介绍X.500、LDAP等所有技术缩写名词的含义）。

ADS为人们在当今不断变化的计算机领域中提供了强大的功能和灵活的使用，但是这些也需要一定的代价。其中最大的部分就是系统管理员将需要深入地学习相关技术，才能够完全理解和使用微软公司开发的Windows 2000和Active Directory Services的潜在功能。

最早商业化的以目录服务为基础的操作系统是Novell公司开发带有NetWare Directory Services（NDS）的NetWare 4系统。在该系统问世的时候，我在美国明尼苏达州的Minneapolis一家公司任高级技术指导。为了在竞争中占据有利位置，我所在的公司派我去学习该系统β测试版的预备课程。经过两星期的NDS全面培训回到家后，我开始重新考虑自己的事业选择。我感到似乎以前自己所掌握的一切都是过时的，我必须掌握一种新型的技术，它就叫“目录服务（directory service）”。必须承认，当我第一次接触到Novell公司的目录服务时我并没有掌握它，并且没有想过自己是否会掌握也不知道自己是否愿意去掌握。在学习NetWare的早期版本时，我仍然有一种安全感，而且不能理解为什么会有人想在自己的网络中加入这么复杂的技术。

但愿本书能够帮助读者避免在了解微软公司的最新技术——Windows 2000 Server和Active Directory的时候产生震惊的感觉。网络目录对于连网技术虽然是一项新事物，但人们可以想一想网络技术的最基本方面，不论是Windows 2000、ADS还是别的事物，也只不过是从一个领域到另一个领域的技术发展罢了。人们已经掌握的所有知识都仍然有效，只是比以前多了一些可选用的内容而已。

浅谈β测试版软件

读者可能已经注意到，微软公司目前还没有发布Windows 2000 Server。编写本书的基础是NT 5系统β2测试版具有的功能。我认为β版软件是“还未准备好投入主流应用”的代码。β版软件提供了两种十分重要的服务：

- 它使公司能够让无数用户在软件投放市场之前对软件进行测试。我也曾经是一名软

件开发人员（当然开发的项目比此小得多），我知道在软件开发过程中最困难的工作之一就是预测软件可能出现的应用条件。开发者在自己小小的实验室中进行测试是一种情况，但不意味着任何人都可以在自己的设备上良好地进行使用！软件投入实际应用时，会在成千上万种不同类型的硬件上运行，有些甚至是开发者闻所未闻的。这样的情况简直就象是玩弹球游戏那么不可琢磨。这里谈到的“实际使用”测试就是β测试所经历的过程。软件开发出来并不是要在一种生产环境中使用，参与β测试的用户要模仿各种可能的“真实环境”对软件进行测试。每当听到有人说“我曾经尝试过β测试，令人大失所望！”这样的话时，我都会忍不住想笑。这就是β版软件可能出现的结果——它还没有真正准备好。这就是β版的定义！

- β版程序还可以在人们试图实现某些计划之前，先为人们提供学习软件的机会。我已经不记得有多少次，就因为一篇商务周刊上的文章——公司的某个副总裁穿越全国，只为参加一个下午2:00的茶会在飞机上读到的，就要求我安装一个软件！通常这些要求都是因为一家有一个巨大的销售部的公司开发了一种新软件，不知读者是否也有这种体会？奇怪的是有些人会在微软公司的Windows 2000 Server刚一上市就安装这种系统，也不管自己是否已经准备好进行这种安装！β版软件使人们在要求正式使用软件（或提供支持）之前能够了解软件自身的功能和弱点。这也是编写本书的目的：在公司的老板要求工作人员在实际使用的工作网络上安装Windows 2000 Server之前，让技术人员先学习Active Directory具有的功能。

当然，以β版软件为基础编写本书也存在一些缺点。编者无法确定自己在β版中了解的情况是否会在最终上市的版本中原样出现。在开发和测试过程中，开发者经常会认识到他们最初的功能表过于夸大，因此最后会去掉一些原计划要发表的功能，或者把一些功能推迟发表。

当Windows 2000最终面市之后，我还会对本书做一些修改。在此之前，本书可以作为一种前瞻性的作品，对微软公司计划在Windows 2000中推出的技术进行介绍。

实际上，Active Directory是Windows 2000系统环境中的关键组成部分，我认为ADS的功能不会有任何重大的变化。至多在此后计划推出的Mastering Active Directory（《Active Directory从入门到精通》）后续版本中会采用一些新制作的屏幕捕获插图，以说明ADS和Windows 2000 Server的“外观和使用感觉”。

内容安排

在编制本书的内容时，我竭尽所能地向读者展示微软公司的最新网络方案——网络目录的概念。也曾经有人建议只编写与Active Directory Services相关的内容，其它方面听之任之，但我还是想让读者在了解ADS的同时对这种技术有一个整体的认识。我把全书分为三部分以实现这个目标，下面是对各部分的介绍。

第一部分：网络目录的背景和历史

不论微软公司如何进行宣传，网络目录实际上已经出现了相当一段时间。理解这种技术的早期实现形式有助于人们理解ADS的工作过程——也许还有助于人们认识其中的一些弱

点。第一部分内容很短，但包含了许多概念性内容，对于读者根据自己的工作环境认识ADS大有裨益。第一部分包括四章。

第1章：网络目录简介　这一章对什么是网络目录作了基本介绍，并与一些过去使用的技术进行了对比。

第2章：网络目录剖析　读者将通过一些现有技术实例在这一章学习什么是网络目录，从最基本的书面目录开始，逐渐进入当前使用的网络系统。

第3章：X.500推荐标准　这一章概括介绍了X.500推荐标准，它用于生成Active Directory数据库的结构。

第4章：网络目录的访问　第4章介绍DAP和LDAP，这是两种用于访问ADS数据库信息的协议。

第二部分：微软Active Directory Services

当读者对目录技术有了牢固的基础知识，就可以接着以一种审视的态度学习ADS，寻找它的优点和弱点。有了这些信息，我们就可以更好地把学到的技术应用在自己的工作环境中。第二部分一共九章。

第5章：没有ADS的微软NT系统　为了全面地了解Windows 2000 Server，特别是Active Directory Services，理解早期的NT版本很重要。如果读者是一位NT系统的专家，可以把本章作为一个复习。如果读者是NT领域的新手，本章会介绍一些在本书后面的阅读中将会遇到的主题。

第6章：带有ADS的微软NT系统　正象NT系统当初设计出来是用于克服以服务器为中心的环境存在的弱点那样，带有ADS的Windows 2000 Server的设计是为了克服基于域的环境存在的弱点。本章将讨论ADS如何融入Windows 2000的总体思路之中。

第7章：基础知识入门　ADS、TCP/IP、DNS、WINS，虽然微软公司的Windows 2000 Server可以使用许多种不同的协议进行通信，但ADS需要依靠TCP/IP。在用户安装和配置ADS环境之前，必须对TCP/IP工具和技术有扎实的基础。

第8章：建立Active Directory树形结构　本章介绍设计稳固的ADS结构，并且不对任何网络单独部件构成压力的理论。

第9章：实现自己的设计　本章介绍ADS的安装和建立ADS结构的机制。

第10章：保护Active Directory数据库　如果ADS数据库希望在网络上获得实际应用的话，那么其中存储的信息必须保证安全。本章讨论Windows 2000 Server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工作组中的计算机用户规定用户或计算机的设置。因此，这些内容对于管理基于Windows 2000 Server网络的管理员十分重要。在第11章中，本书将讨论组策略的概念，并且介绍实现这些概念的过程。

第12章：修改Active Directory方案　ADS数据库中包含着对象类，这些类定义了网络资源的类型，而属性则定义了这些类的参数。缺省的类和属性可能对于部分环境并不完全。第12章讨论扩充ADS数据库设计以包含自定义对象类和属性的过程。

第13章：理解和控制ADS站点和复制　对于任何操作系统，不论我们设置的结构多么

符合逻辑，也不论制定的图形化界面多么直观，一旦工作完成了，所有的数据都要通过“管道”来传递。第13章将在考虑可用带宽和通信开销的情况下介绍设计问题。

第三部分：Active Directory Services的将来

这是本书最后一部分，我尝试以个人的眼光来预视一下ADS可能对网络行业方方面面带来的冲击。最后这一部分包括三章。

第14章：ADS和BackOffice 似乎ADS将成为微软网络的主要阵地，因此，它将对微软公司的其它网络产品带来巨大的冲击。第14章将考察ADS可能对Microsoft Exchange Server（微软信息交换服务器）、Microsoft Proxy Server（微软代理服务器）、Microsoft Site Server（微软站点服务器）、Microsoft Systems Management Server（微软系统管理服务器）、Microsoft SNA Server（微软SNA服务器）和Microsoft SQL Server（微软SQL服务器）造成的影响，这些软件构成了人们通常所说的BackOffice Suite（BackOffice组件）。

第15章：ADS和第三方产品 有无数的公司为NT网络环境提供产品以增加或提高其性能。随着微软公司向以目录为基础的操作系统的转移，这些公司将不得不随着转移。第15章将介绍第三方厂商为了跟上微软公司的网络发展的规划而不得不进行的改变。

第16章：Directory-Enabled Networks（具有目录功能的网络，DEN） 目录服务数据库的设计是为了存储关于网络资源的信息。网络的基础构件——路由器、交换器、网关等不过是所管理的另一组资源。本章将讨论网络目录对这些资源的管理造成的冲击。

谁应当阅读本书？

本书针对的读者是具有一定经验并且希望了解微软公司提供的最新技术的网络管理员。本书在此认为读者对网络已经具有一定水平的总体认识，但是还不了解（或了解得很少）基于网络目录的技术。因此如果读者具有一定的微软Windows NT系统工作经验并且很想提前了解Windows 2000，则本书是你的最佳选择。

目前正在使用其它网络操作系统的用户可能也会对这本书感兴趣。在计算机领域似乎无论微软公司做出哪些举动，都将带动整个行业朝该方向的发展，而现在微软公司正在大刀阔斧地迈向网络目录技术！如果用户目前使用的操作系统还未实现网络目录技术，则可以确信一旦微软公司普及这项技术之后，这些操作系统也将转向网络目录技术。而如果用户目前使用的网络操作系统已经采用了网络目录，则可以确信在不久的将来，自己所使用的系统将必须能够与微软Active Directory实现通信。

笔者相信，最终会出现这样一种情况：如果人们现在已经连网并且计划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技术。本书的目的就是向人们提供为了理解和实现微软公司对这项技术的解释而需要的信息。

小结

微软公司的Windows 2000 Server将在网络技术领域掀起又一次巨大的浪潮。一旦该产品问世，人们将必须重新思考自己应该对网络资源和服务赋予何种特性。而在该产品发布之前对这种操作系统的功能进行学习的人也会在该产品问世之后受到人们的羡慕。因此，领先一步就会更好地走向事业的成功。

最后提一句忠告：享受新技术。新技术可能会让人振奋、富有挑战性和十分有趣，但是如果人们过份去抱怨新技术而不是去欣赏它，则可能就离休假的时候不远了！

与本人编写的其它书目一样，如果读者对书中的内容有疑问或者建议，请通过如下电子邮件进行联系：bking@royal-tech.com。笔者期盼着读者的来信。

目　　录

第一部分　网络目录的背景和历史

第二部分　微软Active Directory Services

第三部分　Active Directory Services的将来

第一部分 网络目录的背景和历史

第1章 网络目录简介

计算机业，特别是网络领域，产生的缩略语、术语、短语和时髦用语比其它任何领域都要多。二十世纪九十年代即将流行的词语就是网络目录（network directory）。目录一词没有什么新鲜的，从六十年代这个词就以各种形式出现了。但是现在，这个词即将融入微软公司人们等待已久的Windows 2000 Server系统Active Directory Services（主动目录服务，ADS）之中。为了从这项技术中获得最多的收益，人们必须对目录是什么、不是什么及如何用于简化网络的管理有透彻的理解。这就是编写本书的目的——为读者提供充足的信息以实现、管理和使用微软公司通过Active Directory Services（ADS）提供的服务。

基于PC机的网络已经成为企业应用领域中一个不可缺少的组成部分。它们最初是为了共享一些物理资源的简单解决方案，如共享硬盘空间、打印机等。随着时间的推移，网络已经成为一项十分复杂——经常跨越多个地理位置、把成千上万的用户与大量资源连接在一起的事物。现在，网络几乎控制着从薪金信息到电子邮件通信、从打印机到传真服务的任何工作。随着网络提供的服务的增加，因此也需要越来越多的管理。对管理需求的控制，使网络更容易管理和使用就是目录服务的最终目的。

1.1 理解网络目录

为了理解和欣赏目录服务解决方案的强大威力和易用性，读者必须理解这项技术将要替代的技术。在目录服务出现之前，多数网络操作系统（NOS）都是“基于服务器”的系统。也就是说，多数帐户管理工作都要一台一台服务器地逐个进行。在旧式NOS软件中，每台服务器都维护着一个用户清单，其中记录了谁可以访问其资源（accounts database，帐户数据库）及用户的许可权（Access Control List或ACL，访问控制列表）是什么。如果某个系统有两台服务器，则每台服务器都有一份独立的帐户数据库，如图1.1所示。

可见，图1.1中的每台服务器都要维护一份自己的授权用户列表，并且管理各自的资源。这种系统虽然很简单、易于理解，但是如果系统增长到一定程度，就会复杂得无法控制。假设网络中有250台服务器，共1000名用户，则用户和资源列表就会长得让人感到无所适从！为了避开这种缺陷，一些NOS软件如微软公司的NT 4系统，就配置成允许一些小型的服务

器工作组共享一份用户列表（称为中央帐户数据库），根据这份列表完成系统安全保护和认证过程，如图1.2所示。这种中央帐户数据库为系统管理员提供了对整个网络部分的集中管理地点，称为域（domain）。然而，这种系统当发展到一定程度后也会变得笨重不堪。

图1.1 基于服务器的NOS

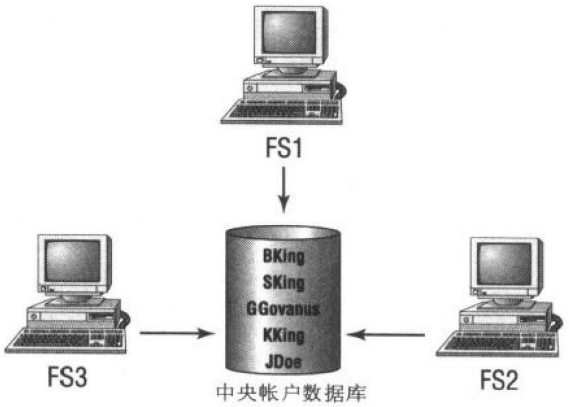

图1.2 NT 4 Security （NT 4安全）帐户数据库

网络从以服务器为基础发展到以域为基础完成了生成一个独立的数据库实现全部用户和资源管理环境的每一步。在域中，所有用户信息都存储在一个独立的地方，并且使用一组工具进行管理，用户可以通过单一的帐户访问网络（不再需要记忆多个用户名和口令）。网络目录则把这一过程继续向前推进一步：实现通过单一的数据库存储整个网络中的全部用户和资源信息。

注意： 本文使用“用户和资源”一词来指目录数据库中的记录，因为在传统的系统管理员眼中网络应用就是这么回事：用户访问资源。在基于目录系统的环境中，用户只不过是另一种资源而已。这种思想方法上的转变对于理解基于网络目录系统的强大功能十分重要。随着读者对目录概念理解的不断深入，就会对两者的区别越来越清楚。

网络目录就是存储网络信息的数据库。它们可以存储许多种不同类型的信息：

- 用户帐户信息（登录名、口令、权限）
- 用户个人信息（电话号码、地址、雇员ID号）

- 外围设备配置信息（打印机、调制解调器、传真）
- 应用程序配置信息（桌面系统参数、缺省目录）
- 安全信息
- 网络基础设施配置信息（路由器、代理服务器、因特网访问设置）

只要人们能够想得到的，网络目录中都可以存储。

一旦把这些信息集中存储在一个标准数据库中，就可以有多种不同的使用方法。其中最普通的是供系统管理员用于网络访问控制和网络资源访问控制。目录将成为对许多网络活动进行集中控制的地方。下面是其控制的一些过程的例子：

- 当一名用户试图登录进入一个网络时，客户软件会向目录系统发出认证请求。目录服务将判断帐户名是否合法、检查用户输入的口令是否正确，并且检查该帐户附带的权限以判断是否应该允许这次登录请求。
- 一旦一名用户登录进入了系统，他每次访问一项网络资源时，系统都会向目录服务发出查询，目录服务会对查询请求进行判断决定该用户是否具有使用相应资源的权限。目录系统还会为客户返回所请求资源的物理地址。
- 个人用户可以使用目录服务存储个人设置信息。每当一名用户登录进入网络时，他的桌面环境设置、缺省使用的打印机、主目录位置甚至连应用程序图标都可以下载到该用户目前使用的计算机上。用户不需要在每次使用一台新计算机时都重新生成自己的环境。只要用户愿意，其所有环境设置都可以进行集中存储和控制。
- 随着目录技术的日益成熟，人们可以使用该技术通过一些网络设备监视和控制网络传输情况。例如，当一名用户试图访问一个远程网络时，人们就可以通过系统目录确定该用户的请求是否合法。假设系统控制因特网访问所使用的工具与控制其它安全设置的工具相同，或者也许目录系统可以查询不同的设备以确定通向特定网络目标的最通畅的路径。人们甚至可能为特定用户、工作组、应用程序或服务授予较高的网络优先级，保证某些部件提供特定级别的服务。

1.2 传统网络与网络目录的对比

许多目录任务都会从网络目录的功能中受益。许多早期网络存在的最难解决的配置问题在使用网络目录作为集中控制方式之后都会变得易如反掌。

1.2.1 普通管理任务的传统网络解决方案

为了帮助理解，我们考虑一些普通的连网任务和相应的非目录方式解决方案。这些情况都是笔者曾经遇到的实际应用中的网络。读者将会看到，基于非目录技术的解决方案经常会变得十分荒唐。有些情况下，提供的服务无法判断提供用户要求的解决方案需要多少时间。也就是说，传统管理技术对网络的束缚经常限制网络系统实际能够提供的服务。

场景1：信任还是不信任

某公司的市场部门有一台彩色热蜡式图形打印机，公司用于生成质量达到照片水平的宣传手册。由于这种设备的耗材很贵，大约是每页3.00美元，因此公司对哪些人允许使用此

打印设备十分关心。幸运的是，市场部本身是一个域，因此安全性很容易得到维护。在工程部门，用户Susan觉得需要使用这台打印机打印一份图形的原稿，现在需要管理员设置适当的权限。

在具有多个域的环境中，有两种解决这个问题的基本途径：

- 管理员可以在市场部门所在的域与工程部门所在的域之间生成一个信任关系，在工程部门域中生成一个全局工作组，在其中加入Susan的帐户，然后把该全局工作组在市场部门域中设置为适当的本地组。这种解决办法虽然能够让Susan满意，但也意味着系统管理员现在必须跟踪另一个信任关系，更不用说还有相关的本地工作组和全局工作组。
- 管理员可以为Susan在市场部门域中生成一个本地帐户，并且教Susan以“Connect As（作为……连接）”方式使用打印机。当然，这样就会失去一种多域设计的重要优点——一名用户进行一次登录。

场景2：Joe在哪里？

公司的一位主管通知管理员说，有人发现一位名叫Joe的销售部门人员在讨论机密信息，其中包括公司未来的产品设计和市场策略。这位主管想知道Joe都在网络环境中的哪些部分拥有权限及其如何获得的这些权限。她还想让管理员确保Joe只拥有作为一名销售人员应该拥有的权限。

在多域环境中，解决这种问题十分困难。管理员首先想到的可能就是删除Joe的帐户，然后重新建立一个——同时还要保证其它销售人员也只能得到适当的权限。管理员还必须跟踪Joe所属的每个工作组，检查每个工作组的权限，对每一个全局工作组，管理员还得检查他属于哪些本地工作组（包括位于其它域中的本地工作组）。管理员还要搜索市场部门和R&D域中所有可能为Joe生成的本地帐户。最后，管理员可能想生成一份审计策略以跟踪有哪些人在访问机密数据。

注意： 这里假设管理员拥有上述网络环境中其它管理员级的权限，否则还必须与其它系统管理员协商可以采取的步骤。

当管理员完成搜索之后，可能要在全公司范围使用一项策略，确定用户权限该如何授予、哪些用户能够对各种不同类型的资源授予权限及诸如全局工作组和本地工作组的命名标准是什么（这样会使今后的搜索工作容易一些）。在多域环境，实现这些策略的过程简直会是管理员的一场恶梦。

场景3：信息搜索

公司里一台价格昂贵的关键业务打印机突然不打印了。管理员知道这台打印机是前不久刚刚购买的，但是现在需要找到其销售商的联系信息。在传统的办公室中，管理员必须与采购部门联系。采购代理则要在成堆的购货单中通过产品序号或购货的大致日期寻找相应的购货单。如果一切顺利，购货单上会有购买打印机的支票号、购买日期及销售商的名字。有了这些信息，就可以与销售商通话协商维修或更换事宜。