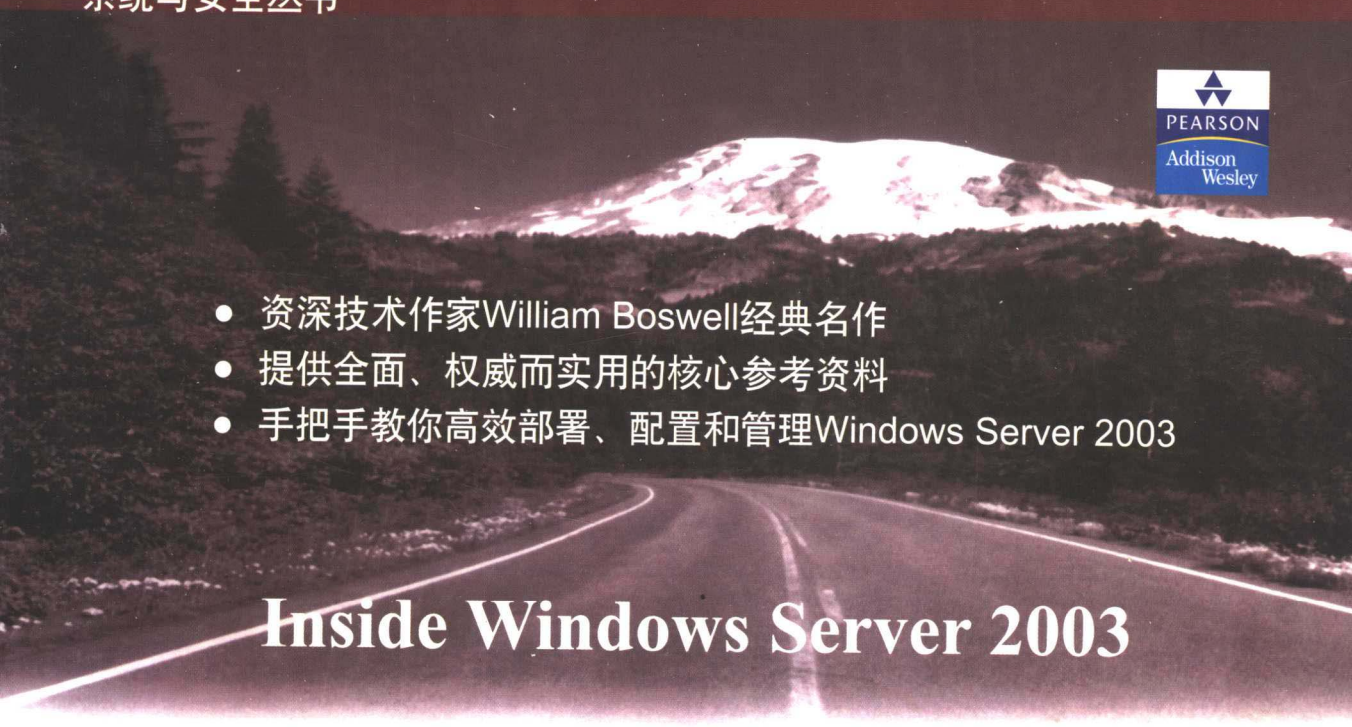
系统与安全丛书



Windows Server 2003 技术内幕(提高篇)

(美) William Boswell 著
周 靖 尤晓东 译

清华大学出版社

系统与安全丛书

Windows Server 2003 技术内幕

（提高篇）

（美）William Boswell 著

周 靖 尤晓东 译

清华大学出版社

北 京

内 容 简 介

这是一本全面、权威的 Windows Server 2003 参考手册（分“基础篇”和“提高篇”），作者根据自己多年积累的丰富经验，以生产环境为背景，按照一种合理的编排体系，透彻介绍了该系统的 200 多个新增特性，并介绍了相应的配置过程。“基础篇”涵盖了 Windows Server 2003 的基础知识点，“提高篇”深入系统内部，揭示幕后原理。

本书是 IT 从业人员的理想参考书，也可用作 Windows Server 2003 认证考试的培训教材。

北京市版权局著作权合同登记号 图字：01-2003-4347

图书在版编目（CIP）数据

Windows Server 2003 技术内幕. 提高篇 /（美）鲍斯威尔（Boswell, W.）著；周靖，尤晓东译.—北京：清华大学出版社，2005.2
（系统与安全丛书）
书名原文：Inside Windows Server 2003
ISBN 7-302-10332-1
Ⅰ.Windows… Ⅱ.①鲍… ②周…③尤… Ⅲ.服务器—操作系统（软件），Windows Server 2003 Ⅳ.TP316.86

中国版本图书馆 CIP 数据核字（2004）第 003270 号

出 版 者：清华大学出版社 **地 址**：北京清华大学学研大厦
http://www.tup.com.cn **邮 编**：100084
社 总 机：010-62770175 **客户服务**：010-62776969
文稿编辑：文开棋
封面设计：陈刘源
印 装 者：三河市春园印刷有限公司
发 行 者：新华书店总店北京发行所
开 本：185×260 **印张**：37.25 **字数**：881 千字
版 次：2005 年 2 月第 1 版 2005 年 2 月第1 次印刷
书 号：ISBN 7-302-10332-1/TP・7033
印 数：1～4000
定 价：64.00 元

译 者 序

技术的发展日新月异，著名的 Windows 服务器操作系统也不例外。最新一代的 Windows Server 2003 作为 Microsoft 公司的一个战略性产品，在它的前身 Windows 2000 的基础上进行了全面的改进。无论在安全性、可靠性、可用性，还是在可扩展性方面，新的操作系统都更上了一层楼。

但是，新技术的问世总是为习惯了原有技术的人带来困扰。无论是以前的 Windows NT/2000 网络管理员，还是准备新建一个网络的管理员，都对新的操作系统充满了好奇和疑虑。新的操作系统适合我吗？安装、升级、迁移过程中遇到问题怎么办？我是一个新手，想一开始就使用 Windows Server 2003，有谁能带我入门？

为了满足这一部分人以及那些准备参加 Windows Server 2003 认证考试读者的需要，清华大学出版社引进并委托我们翻译了这本可谓“包罗万象”的《Windows Server 2003 技术内幕》。任何需要设计、管理或者使用 Windows 技术的 IT 专家都应该评估 Windows Server 2003 的新特性。本书将帮助你完成这个评估过程。如果计划安装一个或多个特殊用途的 Windows Server 2003，或者计划升级到 Windows Server 2003 Active Directory，本书将指导你准备部署，并解决中途可能遇到的各种问题。

作为前美国海军核能工程师，本书作者 William Boswell 先生对技术的严谨有着狂热的追求。与此同时，因为以前有过在核电厂担任系统管理员的经历，所以他有一个现成的、面向大型企业的计算机网络可供实践。在此期间，他和他的管理员团队积累了丰富的网络实战经验。通过团队协作，他们确保了这个大型网络的正常运行，并受到了网络用户们的一致好评。

作者的经验在这本书中得到了充分的反映。当你使用 Windows Server 2003 来组建一个网络时，可能遇到的任何问题都能通过本书来解决。除此之外，作者还在书中发表了许多睿智的见解。所有这些都有助于你使用新的 Windows 服务器操作系统，快速地搭建或者迁移本单位的网络，确保网络服务无中断或者只中断短暂的时间，同时为用户们提供良好的网络使用体验。

由于本书知识点众多，本书将分为上、下两册出版。上册是“基础篇”，我们将带领你逐渐认识 Windows Server 2003 操作系统本身以及 Active Directory 域的计划和部署。首先讲述了 Windows Server 2003 作为 Microsoft 最新一代的服务器操作系统所具有的特点，Windows NT/2000 管理员需要注意哪些问题，如何安装和配置操作系统，如何升级和自动安装，新操作系统对硬件有哪些要求，如何添加硬件，如何管理 NetBIOS 名称解析，以及如何管理 DNS 等。接着从第 6 章起，正式进入 Active Directory 的世界，从它的概念开始，细致地讲解它的计划、部署和维护。

本书的下册是“提高篇”，着重讲述了 Windows Server 2003 的安全性和组策略，并探讨了如何对数据存储、文件系统、共享资源、文件加密、PKI、用户工作环境、远程访问

等进行管理。最后还讲述了如何从系统故障中恢复。

本书翻译过程中，译者与原作者进行了积极而卓有成效的沟通。借助于网络的便利，原书存在的所有问题都能迅速得到解决。在这些问题中，大多数都跟原书基于 Windows Server 2003 测试版有关。要注意的是，你现在看到的译本已经基于“Windows Server 2003 简体中文企业版”进行了全面的修订。除此之外，在征得原作者同意的前提下，译者还对原书的许多错误或疏漏进行了修订，并对少数不恰当或不准确的文字及插图进行了修改。所有这一切努力的结果就是，使我们的中译本无论是质量还是风格上，更能满足读者的需求。

本书翻译过程中，如果没有朋友们的参与，我们是无法独立完成这部著作的翻译的。他们是文瑞、胡辉、肖波、胡联庆、文开阳、任涛、苏星兰、张翼。在此向他们表示衷心的感谢。此外，还要感谢周子衿和尤玮秋，她们天真可爱的笑容是我们工作的动力。

周靖　尤晓东

前　言

一个操作系统的新版本的发布，总是伴随着这样或那样的问题。值得花费时间和精力来更新吗？有什么潜在的问题？怎样准备测试和评估，怎样部署？对 Windows Server 2003 来说，这些决策显得尤其复杂，因为 Windows Server 2003 并不是在 Windows 2000 基础上彻底改头换面来的。相反，新版本操作系统只是集成了众多或大或小的改进，而你需要评估所有这些改进——既要单独评估，也要将其作为一个整体来评估，最终才能判断是否值得升级！

在 Microsoft 公司的基于 NT 的产品线中，Windows Server 2003 是历史上第一次将台式机代码和服务器代码分开来发布。Windows Server 2003 产品进入市场时，XP 已经上市了一年多的时间。所以，为了部署 Windows Server 2003，你需要知道怎样管理 Windows Server 2003 和 Windows 2000/NT 服务器的复杂组合，这些服务器可能要由多达 6 种不同的 Windows 客户端来访问（姑且不论大量的第三方客户端）。

本书旨在指导你在一个混合型的工作环境中，完成一次完整的 Windows Server 2003 部署。首先要安装一个独立的服务器，然后顺理成章地升级附加的服务器、安装硬件、处理名称解析、部署和集成 Windows Server 2003 DNS、安装和配置 Active Directory，以及让授权客户端访问基于 Windows Server 2003 的资源（无论是通过局域网来访问这些资源，还是通过 Internet 来访问）。Windows Server 2003 的发布是一个里程碑式的事件，因为它标志着 Microsoft 最后终于开始全面地关注安全问题。鉴于此，本书特别强调了新的安全特性。

每一章都采用固定的编排结构，首先是设计原理，然后是操作说明，帮助你认识互操作性问题，最后是安装和配置本章描述的 Windows Server 2003 特性的具体过程。每一章开始都提供了一个 Windows Server 2003 新特性列表，并强调对 Windows 2000 的显著改进。有经验的 Windows 2000 设计师和管理员可以将这个列表用作指导自己进行评估的一览表。

之所以采用这种方式来描述 Windows Server 2003 的特性，是因为我以前担任过美国海军核电站操作员。为了确保核电站的正常运转，只知道怎样操作单独一种设备是不够的。你必须知道设备的每一项设计元素的原理，这个设备怎样集成到电站这个整体中，以及设备在出现故障时会对电站产生什么影响。幸运的是，借助多年来积累的经验，我深刻地理解一组操作员如何才能高效率地协同工作。他们应该彻底了解自己所控制的设备，除了能让复杂的系统平稳地运行，还应该经常总结经验和窍门，使自己和他人的工作变得更容易。希望本书能使你积累更多 Windows Server 2003 的使用经验，最终在你的 IT 部门组建一个具有同样高效率的工作团队。

本书面向的读者

任何需要设计、管理或者使用 Windows 技术的 IT 专家都应该评估 Windows Server 2003

的新特性。本书将帮助你完成这个评估过程。如果计划安装一个或多个特殊用途的 Windows Server 2003，或者计划升级到 Windows Server 2003 Active Directory，本书将指导你准备部署，并解决中途可能遇到的各种问题。

如果你已经迁移到 Windows 2000，或者正准备向 Windows 2000 迁移，同时希望知道 Windows Server 2003 是否能给自己带来更多的好处，那么每章开头的“新特性”一览表将帮助你了解需要评估的重点。本书对于所有级别（尤其是 IIS）上的安全性都给予了特别关注。我们重点讨论了以下项目的改进：Windows DNS，Active Directory 复制、林与林的信任关系、新的 Active Directory 迁移工具（ADMT）、用于管理组策略的集成“策略的结果集”（Resultant Set of Policies，RSoP）工具。除此之外，还讨论了以下项目的一些重要的新特性：终端服务、加密文件系统（EFS）、公钥基础结构（PKI）以及分布式文件系统（DFS）。我还会请你特别注意在性能、稳定性以及内存控制上的一些总体性改进。

为了升级一个大型基础结构，肯定会花费不少时间和金钱，但在升级到 Windows Server 2003 之后，它所带来的好处也是非常可观的。这种系统更快、更容易管理，你的用户也能体验到更快的速度和更大的方便性。

本书不面向的读者

本书假定你具有 Windows NT 服务器和经典 NT 域的经验。如果你具有其他操作系统的 IT 背景，而且希望刚开始接触新主题就尽可能深入地了解它，那么可以在本书找到充足的背景解释以及其他参考资料，它们将指导你熟悉几乎一切主题（但最困难的一些主题除外，它们仍然要求你具有 Windows NT 或者 Windows 2000 的背景）。但是，如果你只是希望学习 Windows 和网络技术，最好选择其他书籍。

由于这是一本讲解 Windows Server 2003 的书籍，所以如果你主要关心如何部署和管理桌面，可以参考 Window XP 主题的其他许多书籍（比如 *Windows XP Tips & Techniques* 的中译本《中文 Windows XP 使用技巧》——译者注）。但是，如果你想了解 Windows Server 2003 的服务器端特性如何与 XP 和 Windows 2000 客户端集成，以便对文件夹重定向、脱机文件、组策略、资源共享、名称解析、远程用户访问、证书登记、EFS 以及智能卡等进行有效的故障诊断，那就可以参考本书的详尽描述。

如果你主要关心 Windows Server 2003 资格考试，那么本书提供了让你通过考试所需的大多数信息，但是内容的组织方式有别于传统的考试材料。本书的组织方式更实用，除了能帮助你准备考试，还能使你在以后的工作和学习中更方便地查找参考资料。

由于篇幅有限，本书没有讲解 Internet 信息服务（IIS）6.0 的许多新特性，也没有深入讨论终端服务的“应用程序”模式的许多方面。另外，本书不准备讲解 Novell NetWare 和 Novell Directory Services（NDS）、Services for Macintosh（SFM）或者 Services for UNIX（SFU）的互操作性问题。但是，第 11 章详细讨论了 Windows Server 2003 Kerberos 与基于 UNIX 的 MITv5 Kerberos 的互操作性问题。

本书的约定

本书编排采用以下约定（中译本进行了调整——译者注）：

- 首次出现的新术语要添加引号。另外，根据理解起来的难度，将选择性地添加英文原文——例如，Microsoft 将“站点”（site）定义成一个可靠的、高速的网络通信区域。
- 文件、Active Directory 对象、注册表项和值以及组策略设置的路径采用正常字体——例如，Hosts 文件位于\Windows\System32\Drivers\Etc 文件夹，而 DNS 区域配置信息存储在注册表的 HKLM | Software | Microsoft | Windows NT | CurrentVersion | DNS Server | Zones 中。注意，HKLM 是“HKEY_LOCAL_MACHINE”的简称。
- 需要单击、选择/撤选、勾选/清除、打开/关闭或者特别注意的屏幕元素用中文大括号（【】）来标记——例如，请单击【添加】，打开【添加独立管理单元】窗口。或者，请撤选【桥接所有站点链接】选项，从而移除站点链接删除全局可传递桥接。
- 选择菜单项时，用|符号分隔各个选项——例如，请选择【文件】|【打开】。
- 图形化实用程序使用它的中文化名称（标题栏中显示的名称）。对于具有特殊控制台的命令行实用程序，它们的名称则采用首字母大写的形式——例如，【证书】控制台允许你查看自己的个人证书；为了移除表示已禁用域控制器的对象，你需要使用 Ntdsutil 实用程序。
- 对于标准的命令行实用程序（无特殊控制台），在正文中提到它们的名称时，采取所有字母大写的形式，但在命令行中显示时，采用全部小写的形式——例如，你可使用 IPCONFIG 实用程序从本地 DNS 缓存中清除负响应，格式是：ipconfig /flushdns。
- 在路径和命令中，所有占位符显示成斜体——例如，RUNAS 命令的语法是 runas /u:*user@domain.root* /smartcard。

作者简介

William Boswell，获 MCSE 证书：亚利桑那州凤凰城“Windows Consulting Group”的首席工程师。除了负责培训和咨询，Boswell 还在为 *MCP Magazine* 撰写颇受好评的“Windows Insider”专栏，并且是众多技术会议的广受欢迎的发言人，比如 TechMentor，SANS 和 WinConnections 等。他的电子邮件地址是 bboswell@winconsultants.com。

技术审稿人简介

本书撰写过程中，很多审稿人提出了许多非常宝贵的意见和建议。本书完稿之后，他

们仔细审阅了全书的技术问题和内容编排。在他们的协助下，本书的质量得到了全面的保证，使我们有信心为读者提供最高质量的技术信息。

David Shackelford 是加州 Whittier 市的一名网络工程师。他在 1997 年取得 MCSE 和 MCT 证书，并应 Intel 和惠普公司的邀请，在全国范围内开设 Microsoft 网络和操作系统课程，后来转向对企业网络的研究和实践。他目前受聘于 ChoicePoint 公司，担任首席系统/网络工程师的职务，最近已开始在 Biola 大学讲授 Cisco 技术。

Bob Reinsch 是堪萨斯州 Lawrence 的一名培训专家和咨询专家。他毕业于 Wichita 大学，自 1977 年便开始接触计算机。他获得的证书包括 MCSE、MCT、康柏授权系统工程师和康柏授权培训专家、SAIR/GNU Linux 认证专家/认证技术培训专家以及 Real World Security 的授权培训专家。本书是 Bob 所承担的第 18 个技术编辑工作。Bob 的电子邮件地址是 bob@piercingblue.com。

目　录

第 11 章　理解网络访问安全性和 Kerberos

我以前在一家公司担任过 MIS 总监，该公司运营着一个电话销售中心。销售代表每天要打出去大量电话，他们偶尔会遇到懂得网络安全的顾客。我是怎么知道这一点的呢？因为某些顾客会提出这样一些问题："我怎么知道你就是你说的那个人？"，"我怎么知道你有权把这个东西卖给我？"以及"你介意我录这个电话吗？"。

能提出这些问题，表明顾客熟悉网络安全机制的三大支柱：

- 身份验证
- 授权
- 审计（审核）

销售代表遇到这样"难缠"的对手，往往会挂断电话，转向下一位不那么麻烦的顾客。这从另一个角度证明人们在参加 IT 培训后，在日常生活中也能反映出实际的效果。

本章解释了 Windows Server 2003 如何实现网络安全机制的上述三大支柱。第 18 章将探讨有关"公钥基础结构"（Public Key Infrastructure，PKI）的一些更高级的安全主题。

11.1　Windows Server 2003 新增特性

Windows Server 2003 新的安全机制在功能上有所改进，同时对一些传统的、易受攻击的领域进行了增强。其中包括：

- **新的标准帐户**。新的"本地服务"（Local Service）和"网络服务"（Network Service）帐户将一些服务从具有高度特权的"本地系统"（Local System）安全上下文中移除。这些帐户还为 IIS（Internet Information Services，Internet 信息服务）带来了好处，因为它们允许将一个网站指派给一个非特权帐户。
- **匿名登录**。由于采用新的方式来控制匿名登录，Windows Server 2003 对于 NetBIOS 服务扫描程序具有更强的抵抗力。现在，不再将 Everyone（每个人）组指派给一个匿名连接的访问令牌。
- **身份凭据缓存**。现在，你可以存储辅助名称和密码，以便在访问不在域中的服务器时使用。这简化了对防火墙 DMZ 区域中的服务器以及其他标准服务器的管理。
- **减少了到 PDC 模拟器的通信量**。如果一个域控制器（Domain Controller，DC）不是 PDC 模拟器，同时从用户那里接收到了不正确的身份凭据，它就会在本地缓存结果，从而减少到 PDC 模拟器的通信量。默认情况下，用户最多能发出 10 个转发请求。如果超出这个限制，就在 10 分钟的时间里，拒绝用户根据缓存的信息来访问。
- **对密码重设的处理**。在 Windows 2000 中，一次未经许可的密码重设会使黑客获

得对机器上的加密元素的访问权限，从而为加密文件和安全电子邮件带来危害。Windows Server 2003 禁止了对密码进行未经授权的更改，从而保护了加密结构。

- **对丢失密码的处理**。在忘记本机密码的前提下，一个新的“密码重设盘”特性允许你找回一个独立服务器的密码。
- **简化了领域信任**。Windows Server 2003 采用新方法建立到 MITv5 Kerberos 领域的可传递信任，从而简化了开源领域（open source realm）和 Windows 域的集成。

11.2 Windows Server 2003 安全结构体系

你有必要知道 Windows Server 2003 安全系统的各个组件是如何协同工作的。这样有助于你设计一个安全的系统，并在遇到问题时采取正确的方式加以诊断。图 11.1 展示了安全系统的主要组件，这个安全系统称为“本地安全机构”（Local Security Authority，LSA）。

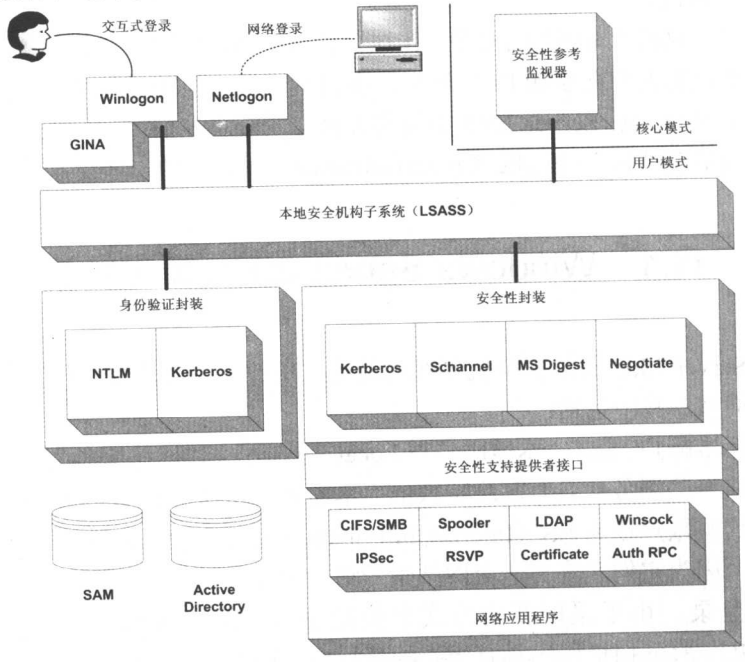


图 11.1 LSA 功能示意图

下面是你看这幅图时要注意的要点：

- 身份验证是通过基于密码的事务处理来实现的，其中涉及 Kerberos 或者经典 NT LanMan（NTLM）Challenge-Response（质询-响应）。安全系统还直接支持不依赖于密码的第三方机制（比如智能卡），并支持包括生理特征检测在内的附加安全机制。
- 实现授权时，Windows Server 2003 使用名为“安全描述符”的特殊数据结构来保护资源。安全描述符指出谁能访问一个资源，以及他们能对这个资源采取什么操作。所有进程都由定义了用户安全上下文的“访问令牌”（access token）来进行

标识。

- 审核由安全系统中的特殊功能来完成，它们能记录对安全对象的访问。

在 LSA 中，包含作为 Windows Executive 一部分来执行的“核心模式”服务，以及对客户端-服务器进程（比如交互式登录和网络访问权限的授予）进行控制的“用户模式”服务。LSA 中的用户模式安全服务包含在两个可执行程序中，即“本地安全机构子系统”（Local Security Subsystem，LSASS.exe）以及 Winlogon.exe。LSASS 容纳着以下进程：

- **Kerberos KDC**。该服务提供 Kerberos 身份验证和票证授予服务。它使用 Active Directory 来存储安全身份凭据。
- **NTLM 安全性支持提供者**（NTLM security support provider）。这个服务用于提供经典 NT 身份验证和安全性管理。它支持所有下级（旧式）客户端以及非域成员的现代 Windows 客户端。
- **安全帐户管理器**（Security Account Manager，SAM）。这个服务负责从 SAM 数据库获取用户身份凭据，以响应来自遗留 NTLM 提供者的请求。
- **Netlogon**。这个服务处理来自下级客户端的“直通”（pass-through）式身份验证，从而提供对经典 NT 身份验证的支持。Netlogon 不支持 Kerberos 事务处理。在基于 Active Directory 的域控制器上，Netlogon 负责注册 DNS 记录。
- **IPSec**。这个服务管理 IP Security（IPSec）连接策略和 IPSec Internet Key Exchange（IKE）。
- **保护性存储**（Protected Storage）。这个服务负责加密并安全存储与 PKI 子系统关联的证书。

11.2.1 LSA 组件

当你从商店购买一套立体声音响时，会和售货员进行一系列事务处理。售货员取得你的信用卡，在一台收银机上刷卡，由机器向另外一个地方的数据库验证这张卡，向你索取签名来证明这一笔买卖，最后包装好你买的商品以便发货。

用一个流程图来描绘购物过程，就能从中轻松地识别出标准的安全元素：身份验证、授权以及审核。其中任何一个元素都可以采取不同的方式来执行，而不会影响到其他元素。例如，如果决定开支票而不是刷卡，那么身份验证步骤就会扩展，加入“查看你的驾照”这一环节。

访问一个服务器上的安全资源时，你会遇到一系列类似的安全事务处理。对这些事务处理进行管理的服务称为“封装”或者“包”（package）。有两种类型的封装：身份验证封装（authentication package）和安全性封装（security package）。

身份验证封装

显然，“身份验证封装”验证的是你的身份。Microsoft 提供了两个身份验证封装：

- **Kerberos**。一种三路身份验证机制，服务器使用由一个可信来源颁发的密钥来验证一个客户端的身份。
- **MSV1_0**。遗留的 NT 身份验证封装（或者称为“NT 认证包”）。通常把它称为“质

询-响应”（challenge-response）身份验证，因为它要求传送一个加密的随机数（称为“质询”）。Windows Server 2003 支持源于 DOS 的客户端（Windows 3.11，Windows 9x 和 ME）所用的 LanMan（LM）质询-响应，以及 NT 客户端和非域成员的现代 Windows 客户端所用的 NT LanMan（NTLM）质询-响应。

经典安全性数据库

NTLM 身份验证将安全信息存储在注册表的 3 个数据库中：

- Builtin。这个数据库包含两个默认的用户帐户：Administrator 和 Guest；另外还有各个默认组，比如用于域的 Domain Users 组以及用于工作站和独立服务器的 Power User 组。Administrator 和 Guest 帐户不可删除，但可以重命名。Builtin 组拥有特殊的操作系统权限，它们不可删除或重命名。Builtin 帐户包含在 SAM 注册表分支中。
- 安全帐户管理器（Security Account Manager，SAM）。这个数据库包含了本地用户和组帐户。在经典 NT 中，一个主域控制器（Primary Domain Controller，PDC）上的 SAM 定义了一个域中的安全实体。SAM 数据库包含在 SAM 注册表分支中。
- LSA。这个数据库包含了计算机的密码规则、系统策略以及可信帐户。LSA 数据库包含在 Security Registry 分支中。这个分支也包含了 SAM 数据库的一个拷贝。

将一个经典 PDC 升级成 Windows Server 2003 时，注册表数据库的大多数内容都会迁移到 Active Directory 中。经典 LSA 数据库中的策略所定义的系统权限与用户权限会被 \Windows\Security\Database 目录下的 Secedit.sdb 数据库所存储的一系列组策略取代。

安全性封装

在一个“安全性封装”中，包含了管理身份凭据访问、保护数据以及保护客户端与服务器之间的消息流时所需的协议及特性。

安全性封装也称为“安全性支持提供者”（Security Support Provider，SPP）。使用安全服务的应用程序无需关心这些提供者的细节。一个“安全性支持提供者接口”（Security Support Provider Interface，SSPI）负责对安全性提供者的功能进行抽象。从概念上说，这类似于“开放数据库互联”（Open Database Connectivity，ODBC）对数据库访问进行抽象，也类似于“网络设备接口规范”（Network Device Interface Specification，NDIS）对网络接口访问进行抽象。

Microsoft 在 Windows Server 2003 中提供了以下安全性封装：

- Kerberos。Kerberos 具有特殊的地位，因为它既是一个身份验证封装，也是一个安全性封装。作为安全性封装，它允许应用程序在访问资源时出示“Kerberos 票证”。这种应用程序称为 Kerberos 应用程序。一个例子是 Windows Server 2003 和 Windows 2000 中使用的 CIFS/SMB 网络文件系统服务（SMB 代表“Server Message Block”，即“服务器消息块”，它是 Windows 网络使用的命令语言。CIFS 代表“Common Internet File System”，即“通用 Internet 文件系统”，它是 SMB 的另一种称呼）。
- NTLM。这个封装用于支持下级（旧式）Windows 客户以及独立的 Windows Server

2003，XP 和 Windows 2000 机器的连接。

- Digest。这是 Microsoft 对 RFC 2617“HTTP Authentication: Basic and Digest Access Authentication”的一种实现。在 Digest 封装中，还包含了对“简单身份验证和安全层”（Simple Authentication and Security Layer，SASL）中的 Digest 身份验证的支持，这具体依据的是 RFC 2831“Using Digest Authentication as a SASL Mechanism”的定义。Windows Server 2003 使用的这个新版本的 Digest 封装允许使用 MD4 密码散列来加密质询，所以避免了使用可逆密码的必要。
- Schannel。这个封装包含了支持私有的、受保护的 Web 通信所需的安全协议。具体包含的安全协议有：“传送层安全性”（Transport Layer Security，TLS），“安全套接字层”（Secure Sockets Layer，SSL）以及“私有通信技术”（Private Communications Technology，PCT）。
- Negotiate。这是一个所谓的“伪提供者”。换言之，它其实不包含任何安全协议。相反，它允许客户端发现可用的安全性封装，并决定具体使用哪一个。例如，一个 Kerberos 应用程序在调用 Negotiate 时，就会自动切换到 Kerberos 封装。

除了上述主要的安全性封装，Windows 还包含以下未在图 11.1 中出现的封装：

- 标准 Digest（摘要式）身份验证
- 明文密码身份验证
- 分布式密码身份验证（用于支持 MSN）
- 旧式 MSN 身份验证

Winlogon

LSA 需要通过某种机制从用户处获得登录身份凭据。负责获取这些身份凭据的可执行程序就是 Winlogon.exe。当你按下 Ctrl+Alt+Del 时，就会调用 Winlogon.exe。

随后会打开一个“Windows 安全”窗口，它也由 Winlogon 控制。如果你还没有登录，安全窗口将提供一个地方让你输入登录身份凭据。如果已经登录，该窗口就提供让你注销、关机、锁定计算机、更改密码或者打开“任务管理器”的选项。

Winlogon 所提供的窗口来源于一个名为“图形标识和身份验证”（Graphical Identification and Authentication，GINA）的 DLL。独立软件开发商（Independent software vendor，ISV）可以替换 GINA，或者对它进行增强，以便捕捉它们自己的身份凭据。例如，Novell 的 Netware 客户端会安装一个定制的 GINA，它能为 Novell 目录服务收集附加的登录身份凭据。

安全性参考监视器（SRM）

将域或服务器想象成一座城堡，将身份验证封装想象成门卫，那么“安全性参考监视器”（Security Reference Monitor）就是城堡里负责保护重要人物的一个保镖队。

注册表提示：安全性封装

安全性支持提供者列表位于 HKLM | System | CurrentControlSet | Control | SecurityProviders 中。

LSA 及其安全性支持提供者的控制参数包含在 HKLM | System | CurrentControlSet | Control | LSA 中。

Windows 为包括 NTFS 文件/文件夹、注册表项、Active Directory 对象、打印机、服务以及核心进程在内的对象提供了单独的安全性。为此，它将每个对象都链接到一个名为“安全描述符”的特殊数据结构。安全描述符中包含一个访问控制列表（ACL），它标识了允许或拒绝访问对象的用户、计算机和组。

用户登录时，LSASS 会构建一个访问令牌，它用于向安全系统描述这个用户。令牌中包含用户的安全 ID（SID）、用户所属的任何组的 SID 以及各种安全策略设置（比如登录过期时间以及密码复杂度要求等）。

由用户所有的一个进程在尝试访问一个安全对象时，“安全性参考监视器”会将安全描述符中的 SID 与用户访问令牌中的 SID 进行比较，并得出用户的访问权限集合。

访问令牌和策略一样，肯定是本地的。它们不能伴随用户在网络中漫游。用户连接到一个服务器时，服务器上的 LSASS 必须建立代表该用户的一个本地访问令牌，以便将令牌附加到用户的进程上。LSASS 通过两种方式之一获取构建这个本地访问令牌所需的信息：

- 如果是 Kerberos 身份验证，它从客户端出示的 Kerberos 会话票证的 Authorization Data 字段中获取信息。
- 如果是 NTLM 身份验证，它从一个域控制器获取信息，这是作为“直通”（pass-through）式身份验证过程的一部分来完成的。

必须对用于构建访问令牌的令牌进行严密的保护。如果黑客劫持了一个访问令牌，或者破解了用于构建访问令牌的机制，那么身份验证系统再怎么强大也无济于事，因为黑客无论如何都能进行访问。

11.2.2 LSA 工作过程概述

本节将暂停更加深入的讨论，简单总结一下迄今为止已经出场的各个“演员”，看它们在由身份验证、授权以及审核这三大支柱搭建起来的网络安全大舞台上，具体是如何配合和表演的：

1. Winlogon 从用户处收集登录身份凭据。
2. LSASS 获取这些身份凭据，并在 Kerberos 或者 NTLM 的帮助下（通过 MSV1_0），使用这些凭据来验证用户的身份。这是“身份验证”阶段。
3. LSASS 构建一个访问令牌，它定义用户的访问权限和系统权限。
4. 安全性参考监视器（Security Reference Monitor，SRM）将这个令牌与对象的安全描述符中的访问控制列表（Access Control List，ACL）进行比较，判断是否允许用户访问。这是“授权”阶段。
5. 最后，LSASS 和 SRM 配合，监视对安全对象的访问，并生成报告来记录部分或者全部访问事件。这是“审核”阶段。

下面让我们详细探讨这些安全性组件，并着重强调配置选项以及潜在的安全脆弱性。