

<<Windows Vista安全管理权威>>

图书基本信息

书名：<<Windows Vista安全管理权威指南>>

13位ISBN编号：9787302178217

10位ISBN编号：7302178216

出版时间：2008-6

出版时间：清华大学出版社

作者：（美）米勒西，（美）海里斯 著，黄广华，张芳 译

页数：305

字数：366000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<Windows Vista安全管理权威>>

### 内容概要

本书主要内容： 讨论了Vista的很多令人惊喜的特性，如以管理员的身份登录以及如何重新启用Run命令 揭示了虚拟化的工作原理 解释即使是管理员也不能删除System32中文件的原因 细述了新的引导后安全特性，如PatchGuard 引入了新的BitLocker特性，以便最大限度地保护便携式计算机 讨论了新的Windows完整性机制 探讨了改进后的事件查看器，事情转发和新的故障诊断工具

## 作者简介

Mark Minasi, MCSE, 世界一流的Windows资深专家, 曾在15个国家授课, 是研讨会和业界集会上的一位颇受欢迎的发言人。

他创立的公司MR&D已教会数万人设计和运行Windows网络。

Mark已经为Sybex撰写了超过15本书, 包括畅销书Mastering Windows Server 2003和The Complete PC Upgrade

## &lt;&lt;Windows Vista安全管理权威&gt;&gt;

## 书籍目录

第1章 Vista安全管理	1.1 恢复Administrator账户	1.1.1 生成自己的管理员	1.1.2 激活Administrator账户
	1.2 Power Users本质上已取消了BOOT.INI	1.3 Start菜单中取消了Run命令	1.4 用BCD取代了BOOT.INI
	1.4.1 boot.ini回顾	1.4.2 BCD术语	1.4.3 创建第二个OS条目
	1.4.4 创建第二个OS条目	1.4.5 用bcdedit选择超时值和默认OS	1.4.6 改变条目选项
	1.4.7 删除OS条目	1.5 取消了Documents and Settings文件夹	1.6 IPv6与网络特性
	1.7 远程桌面更安全	1.7.1 NTFS和Registry以事务为基础	1.7.2 Windows真正有了取消删除的功能
	1.8 安全选项的变化	1.8.1 对命名管道访问的改变	1.8.2 对共享和注册表访问的改变
	1.8.3 不强	1.8.4 不再有未签名的驱动程序告警	1.9 加密
	1.9.1 Vista包含新的加密服务	1.9.2 加密页面文件	1.9.3 每个用户的Offline Files文件夹被加密
	1.10 新的事件查看器	1.10.1 事件查看器中包含XML格式	1.10.2 通过定制查询可以定制事件查看器
	1.10.3 事件查看器	1.10.4 告知事件日志服务显示消息	1.10.5 将事件从一台计算机转发到另一台计算机
	1.10.6 订阅概述	1.10.7 创建一个订阅范例	1.10.8 订阅延迟的故障诊断
	1.10.9 工作组中的事件转发	第2章 理解用户账户控制	2.1 介绍UAC
	2.2 UAC有哪些好处	2.2.1 UAC对用户的好处	2.2.2 UAC对管理员的好处
	2.2.3 UAC是一种转换工具	2.3 UAC概述	2.4 深入挖掘UAC
	2.4.1 Windows如何创建标准用户令牌	2.4.2 如何告诉UAC使用管理员令牌	2.4.3 Windows何时使用管理员令牌
	2.5 重新配置用户账户控制	2.5.1 打开、关闭或进一步驾驭UAC	2.5.2 UAC初级配置：用户的UAC
	2.5.3 必须具有怎样的管理员特征才能获得UAC	2.5.4 排除内置的管理员	2.5.5 告诉UAC跳过试探法
	2.5.6 控制安全桌面	2.5.7 要求签名的应用程序	2.5.8 应对将数据存储在错误地方的应用程序
	2.5.9 完全关闭UAC	2.6 UAC会取得成功吗	2.7 小结
	第3章 文件和注册表虚拟化	3.1 文件和注册表虚拟化基础知识	3.2 文件虚拟化的工作情况
	3.3 文件和注册表虚拟化需要考虑的事项	3.4 哪些区域被保护及它们在哪里虚拟化	3.4.1 虚拟化如何处理文件
	3.4.2 虚拟化如何处理注册表	3.5 “遗留”的确切含义是什么	3.6 标准用户与管理看到的虚拟化
	3.7 跟踪虚拟化	3.8 虚拟化存在的问题	3.9 控制虚拟化
	3.10 虚拟化的未来	3.11 小结	第4章 理解Windows完整性控制
	4.1 Windows完整性控制概述	4.2 强制控制与自主控制	4.2.1 橙皮书
	4.2.2 C2级认证和NT	4.2.3 C级和B级：自主与强制	4.3 WIC组件
	4.3.1 WIC的6个完整性级别	4.3.2 对象如何获得和存储完整性级别：强制标签	4.3.3 进程完整性级别
	4.4 了解进程的工作情况	4.4.1 设置	4.4.2 范例：启
	4.4.3 IE浏览器保护模式和WIC	4.4.4 首要指导原则的困惑：WIC和删除	4.5 使用WIC ACE来限制访问
	4.6 WIC ACE不能做的事情	4.6.1 组策略不适用强制标签	4.6.2 不能创建命名强制标签的标准权限
	4.7 修改系统文件的一点说明	4.8 操纵定制标签	4.8.1 SDDL字符串
	4.8.2 探秘B级语言：SDDL标签语法	4.8.3 使用SDDL字符串设置完整性级别	4.9 小结
	第5章 BitLocker：解决便携式计算机的安全问题	5.1 便携式计算机目前存在的安全问题	5.2 BitLocker驱动器加密概述
	5.2.1 BitLocker组件	5.2.2 什么是TPM	5.3 全盘加密
	5.3.1 加密法	5.3.2 密钥存储	5.4 认证或访问控制
	5.4.1 用额外的密钥保护器增强安全性	5.4.2 引导程确认（完整性检查）	5.5 首次启用BitLocker
	5.6 在无TPM的计算机上使用BitLocker	5.7 恢复	5.7.1 恢复范例1：桌面硬件故障（无TPM的独立系统）
	5.7.2 恢复范例2：便携式计算机硬件故障（基于TPM）	5.7.3 恢复范例3：丢失USB密钥（有TPM的计算机）	5.7.4 恢复范例4：“找到的”便携式计算机
	5.7.5 小结	5.8 BitLocker和活动目录	5.9 组策略选项
	5.10 在企业中管理TPM和BitLocker	5.11 为受BitLocker保护的计算机提供服务	5.12 安全退役
	5.13 规划BitLocker的部署	5.14 小结	第6章 引导后保护：代码完整性、新代码签名规则和PatchGuard
	6.1 随机地址空间分配	6.2 64位系统具有更多的保护措施	6.3 代码完整性
	6.4 新代码签名规则	6.4.1 什么是代码签名，它为什么重要	6.4.2 ActiveX控件
	6.4.3 受保护媒体路径的要求	6.4.4 x64的要求	6.4.5 对应用程序或驱动程序进行代码签名
	6.4.6 部署经发布者签名的应用程序或驱动程序	6.5 小结	第7章 Vista如何保护服务的安全性
	7.1 服务简介	7.2 服务控制管理器	7.3 Vista如何加固服务
	7.3.1 会话分离	7.3.2 减少服务权限	7.3.3 服务隔离
	7.3.4 限制服务的网络端口	7.4 小结	



章节摘录

第1章 Vista安全管理本书用很长的篇幅来展示Vista主要的新安全技术是如何工作的，它们对用户产生了什么影响，以及用户如何控制它们。

但本章并未触及这些大的主题，相反，本章要介绍的是Vista的一些变化，这些变化相当有意义，但它们并不是一目了然的，只有在偶尔碰到陌生的、未曾料到的或使人费解的情况时才可能意识到这些变化。

你可能会想“嗨，如果这是令人惊奇的Vista管理和安全的一个小集锦，那为什么不放在本书最后呢？”我想到过这么做，但意识到如果你正在使用Vista的一个副本，并用到了本书其余部分涵盖的一些内容，那么可能会发现与试着攀登内部的用户账户控制（User Account Control，UAC）等高塔相比，更容易被脚下的小荆棘所绊倒，所以在第1章就讲述这些内容似乎更实用。

需要强调的是，这些令人惊奇的变化并不是毫无用处。

本章力图使你能够快速机智地了解在管理方面，尤其是从安全的角度来看，有巨大变化的那些内容，重点强调那些未大力宣扬的变化。

这样就可以确定，对于Windows的这些新变化，最好将时间花费在什么地方。

（另外，我希望能在客户在会议上提到它之前向你展示这些变化。

你不是不喜欢这些变化内容有点出乎意料吗？

）这些内容并无特定的顺序，再次申明，它是一个集锦。

如前言中所述，因为要力图保持本书简短，也因为我正在使用的是Vista的预发布版本，所以继续阅读的前提条件是你已经明白了如何启动Vista，并以最小化的方式运行在一两个测试系统上。

这样，我们就可以继续讨论这些惊奇之处了。

1.1 恢复Administrator账户第一次登录Vista时，你会一如继往地想要以Administrator的身份来登录。

但可能会陷入困境，因为似乎不存在Administrator这样一个账户了。

实际上，Administrator账户依然存在，且可以登录，只是被禁用了。

下面来解释如何恢复它。

首先，以本地管理员的身份登录Vista系统。

如果你处在一个域中，则很可能意味着需要以域管理员账户来登录；如果你不是域的负责人，那么恳请域管理员将你的域账户放到你所用的Vista计算机的Administrators组中。

如果你使用的计算机是域的成员之一，但这两样事都做不到，那就比较麻烦了，除非作为工作组而不是域的一个成员重新安装Vista计算机。

编辑推荐

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>