软件工程师丛书

Admin 911: Windows 2000 Group Policy

Windows 2000 组策略

自救手册

解决问题的方案

修复漏洞的技术

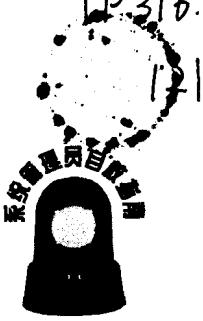
优化性能的方法

〔美〕 Roger Jennings 著

侯国峰 张 岚 程 洁 等译

McGraw-Hill
http://www.mhhe.com

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
URL: http://www.phei.com.cn



软件工程师丛书

Windows 2000 组策略自救手册

Admin911: Windows 2000 Group Policy

[美] Roger Jennings 著
侯国峰 张 岚 程 洁 等译

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

软件工程师丛书

Windows 2000 组策略
自救手册

Admin911:
Windows 2000 Group Policy

[美] Roger Jennings 著
侯国峰 张 岚 程 洁 等译

電子工業出版社
Publishing House of Electronics Industry

内 容 提 要

Windows 2000 的组策略为系统管理员提供了完善的管理手段。本书详细地讲述了使用 Windows 2000 实现的 ZAW-Windows 零管理的功能，包括系统自动更新与应用程序自动安装、所有状态保存在服务器上、集中式管理与系统锁定和应用程序灵活性的最佳方案设计，是系统管理员的必备宝典，也是每个软件工程师值得认真一读的好书。

Roger Jennings: Admin911: Windows 2000 Group Policy,first Edition
ISBN 0-07-212948-4

图书在版编目（CIP）数据

Windows 2000 组策略自救手册/（美）詹宁斯（Jennings, R.）著；侯国峰等译.
—北京：电子工业出版社，2001.4
（软件工程师丛书）
书名原文：Admin911: Windows 2000 Group Policy

ISBN 7-5053-6606-8

Ⅰ.W... Ⅱ.①詹...②侯... Ⅲ.服务器—操作系统（软件），Windows 2000—技术手册
Ⅳ.TP316.86-62

中国版本图书馆 CIP 数据核字（2001）第 18946 号

丛 书 名：软件工程师丛书
书　　名：Windows 2000 组策略自救手册
原 书 名：Admin911: Windows 2000 Group Policy
著　　者：Roger Jennings
译　　者：侯国峰　张　岚　程　洁　等
责任编辑：祁玉芹
印 刷 者：北京市天竺颖华印刷厂
出版发行：电子工业出版社出版　URL:http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编　100036
经　　销：各地新华书店
开　　本：787×1092 1/16　印张：30.75　字数：568 千字
版　　次：2001 年 5 月第 1 版　2001 年 5 月第 1 次印刷
定　　价：48.00 元

书　　号：ISBN 7-5053-6606-8
　　TP・3667

著作权合同登记号　图字：01-2001-0551

出 版 说 明

随着新世纪的到来，人类社会已进入信息时代、网络时代。计算机应用的普及和深入，软件技术的发展和新软件的不断涌现，数量更多质量更高的计算机应用系统的研究和投入使用，要求越来越多的高水平的软件工程师以开拓者的姿态投身其中。

我国的软件工程师队伍已有了长足的发展，软件开发水平已有了长足的进步。作为中国人，我们期盼的是中国软件业走自主创新之路，在世界上的地位越来越高。作为出版工作者，为发展我国的软件事业尽最大努力，是我们义不容辞的责任，这正是我们于 1999 年底推出《软件工程师》丛书的初衷。

目前这套丛书已出版了 20 多种。从市场销售和读者反馈的情况看，这套丛书已经得到了读者的首肯和厚爱，这也是对我们下一步工作的激励。

从当前我国的软件开发情况看，和前几年相比，有了如下变化：

1. 单机单用户应用系统的开发和应用越来越多地转向网络多用户系统的开发和应用，如开发企业网和因特网数据库应用、安全系统等。

2. 单一的高级语言使用越来越多地转向多种高级语言的综合使用，仅仅会用一两种高级语言进行开发的软件工程师已经感到力不从心。

3. 越来越多的软件工程师正在使用一些高级的、包含编程功能在内的应用软件和专用软件，如使用 Flash、Dreamweaver 开发网页，使用 Director、Authorware 开发多媒体演示系统等。

可以说，应用系统的多样化、规模化和复杂化对软件工程师提出了更高的要求，同时也为软件工程师提供了更多的施展个人才华的机会。

针对这种形势，我们正在扩充《软件工程师》丛书的选题范围，进一步界定这套丛书的特色，设想是把丛书按如下类型整合：

一是开发类，通过大量实例说明如何使用各种流行的高级语言、工具类软件开发不同的应用系统，说明开发思想、开发过程、难点及其解决方案。为了适应我国软件工程师开发综合软件系统的需求，我们把包含编程功能在内的高级应用软件的开发应用也纳入到丛书中。

二是技巧类，通过大量实例说明在不同应用系统开发过程中，有关缩短开发周期、提高开发质量、解决开发中的疑难问题的各种技巧。

三是技术类，介绍软件开发的有关理论和技术，以及在实践中的应用，如系统分析与系统设计、软件测试和系统安全等。

四是手册类，即每个软件工程师必备的案头书。

我们把为软件工程师提供图书信息服务为宗旨，坚持以图书质量为生命。我们希望《软件工程师》丛书能对读者有所帮助，希望读者提出更多的宝贵建议和意见，包括工作中遇到的技术难点、疑点和问题。希望更多的作者加入我们的专家行列，推介自己的实践经验和累累硕果。我们的网址是 www.phei.com.cn，请和我们联系。

为了我国软件业的更加美好的明天，让我们共同努力。

電子工業出版社

译者的话

在全球信息化时代，大型企业的内部网络和 Internet 是企业信息系统不可缺少的组成部分。如何在企业内部按照不同部门的职能，如何按照每一个雇员的任务，有效地管理系统的资源和信息，有效地控制谁该获得什么信息，是一项复杂而艰巨的任务。网络越大，服务器和工作站越多，其管理就越复杂。Windows 2000 的组策略提供了比较好的管理手段。

本书由浅入深地讲述了 Windows 2000 实现的 Zero Administration for Windows（ZAW——Windows 零管理）的下列功能：系统自动更新与应用程序自动安装、所有状态保存在服务器上、集中式管理与系统锁定和应用程序灵活性的最佳方案设计。通过一个虚拟大学的例子，具体介绍 Windows 2000 的组网设计和组策略的应用。

本书共分 9 章。第 1 章介绍如何利用组策略管理 Windows 2000 网络；第 2 章介绍如何为组策略的应用设计 Active Directory 拓扑结构；第 3 章介绍如何规划安全组结构控制用户对本地 PC 和网络化资源的访问；第 4 章介绍如何利用 Windows 2000 的一组 Change and Configuration Management(CCM)服务减少网络化客户管理的开销；第 5 章介绍如何应用本地计算机策略；第 6 章介绍如何为具有多个站点的 Windows 2000 域建立策略；第 7 章强调通过组策略建立和维护服务器的安全；第 8 章介绍在 Windows 2000 网络中要考虑到现有的 Windows NT 网络，并实现相应的策略；第 9 章介绍如何将试验环境的组策略配置到产品网络环境中；最后在 3 个附录中有很重要的参考资料。

本书第 1 章至第 9 章和附录 C 由侯国峰翻译，附录 A 和附录 B 由张岚翻译，参加本书翻译工作的还有程洁、宋黎松、段来盛、官章全、李罡、郑城荣、曹恒以及舒智勇等同志。在翻译过程中，除对原文个别错误作了更正外，我们力求忠实于原文。但由于译者的知识水平和实际工作经验有限，不当之处在所难免，恳请读者批评指正。

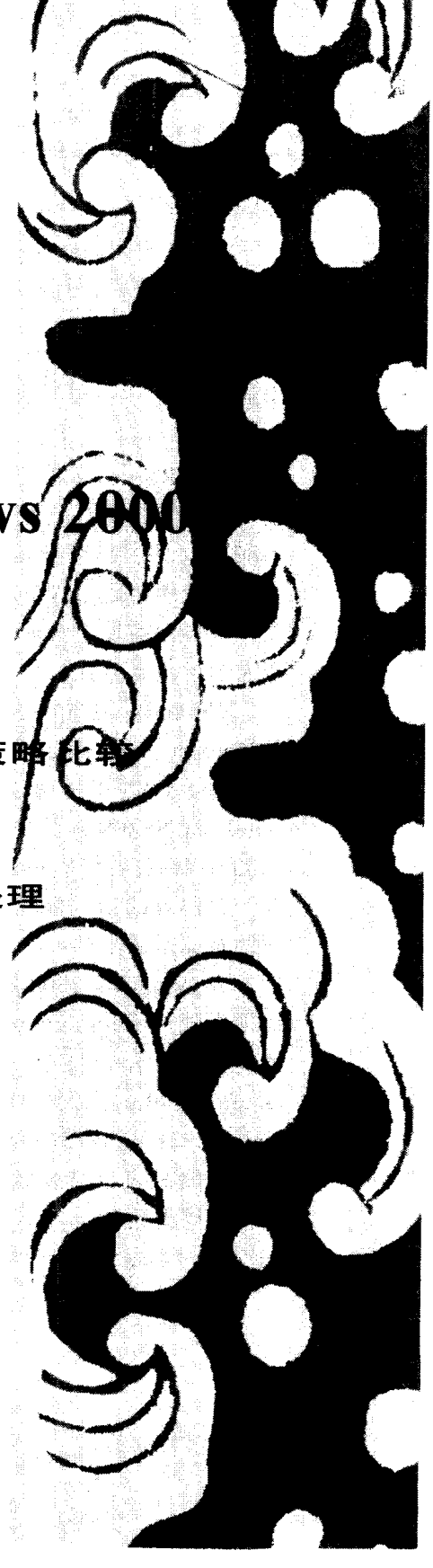
译　者

2001 年 3 月于北京

目　录

第 1 章

使用组策略管理 Windows 2000



组策略(Group Policy)是实现 Change and Configuration Management(CCM——更改与配置管理)Windows 2000 的主要部分，而且是在 Windows 2000 域内部建立一致、有效的安全策略的主要机制。为了实现运行 Windows 2000 Professional 工作站的客户机管理和桌面锁定，组策略取代了 Windows NT 的系统策略。

CCM 包括 IntelliMirror 特性(用户设置与数据管理和软件安装与管理)和远程操作的系统安装。保存在 Active Directory(AD)中的 Group Policy Objects(GPO——组策略对象)和取代 Group Policy Templates(GPT——组策略模板)的 File Replication Service(FRS——文件复制服务)为 CCM 提供基础结构。Group Policy Extensions(组策略扩展)对 GPO 应用安全设置、指定注册和其他脚本以及配置兼容 Windows 2000 的应用软件的自动化安装。

如果希望通过 Windows NT 或 NetWare 升级到 Windows 2000 获得长期的经济效益，就必须实现组策略。业界分析家，如 GartnerGroup 和 Giga Information Group，多数人的意见是升级投资方面的回报完全取决于实现有效的策略管理。

Windows 2000 Server 及其高端产品，诸如 Advanced Server(高级服务器)和 Datacenter Server(数据中心服务器)，都有向导帮助管理员设置其新特性，例如 AD、Dynamic DNS 以及通过 IPSec 运行 L2TP 的 Virtual Private Network(虚拟专用网)。在 Windows 2000 Server 中找不到"Group Policy Wizard"(组策略向导)。组策略是 Windows 2000 最复杂，并在许多方面最违反直觉的特性。如果 Windows 2000 的任何组件应该有一个向导的话，那就是组策略。没有用于建立合理并且一致的 CCM 策略集的内置帮助是编写本书的一个主要原因。

在 Windows 2000 域中不能忘掉组策略。如果在原始安装或 Windows NT PDC 升级期间使用 Dcpromo.exe 创建第 1 个 Windows 2000 Domain Controller(DC——域控制器)，AD 提升过程建立一个应用于该域中所有 Windows 2000 计算机和用户的 Default Domain Policy(缺省的域策略)。AD 的 Domain Controllers 组织单元(Organizational Unit——OU)中的 DCs 接受 Default Domain Controllers Policy(缺省的域控制器策略)。缺省策略只表示组策略历程的起始点，尤其对于一个网络产品来说，基本的域与 DC 安全策略是远远不够的。缺省的本地安全设置对工作站和成员服务器只能提供不牢固的安全。本章中第 1 个组策略管理的例子将描述如何提高域的安全级。

1.1 组策略与 Windows NT 系统策略比较

组策略的前身是 Windows NT 和 Windows 9x 系统策略文件，分别为 Ntconfig.pol 和 Config.pol，它们是用 Policy Editor(Poledit.exe)编辑的。在客户注册的过程中，从 PDC 或 BDC 的 Netlogon 共享加载的这些文件改变客户机 HKEY_LOCAL_MACHINE (HKLM)和 HKEY_CURRENT_USER(HKCU)注册表中的设置。如果已经在一个 Windows NT 4.0 网络中实现(或曾尝试实现)了系统策略，用户将意识到组策略对系统策略的基本 CCM 特性实质上的改进。

系统策略是 Microsoft 于 1996 年宣布首创的 Zero Administration for Windows (ZAW——Windows 零管理)的基础，这是一个修饰矛盾的名称。最初的 ZAW 宣传版(http://www.microsoft.com/presspass/press/1996/Oct96/ZAWinpr.asp)承诺下述特性：

- **自动的系统更新与应用程序安装** 当计算机被引导时，不需要用户的介入，操作系统搜索来自服务器、Intranet 或 Internet 最新的代码或驱动程序。如果这些系统可用，将更新操作系统自身。Automatic Desktop 特性为用户提供所有可以访问的应用程序，当这些应用程序被调用时便自动安装。
- **所有状态保存在服务器上** 用户的数据可以自动地“反映”到服务器上，保证高度的可用性并允许移动用户无论是否连接到网络都能够访问的信息。此外，只要维持对数据、应用程序以及用户化环境的全部访问权限，用户将能够在 PC 之间漫游。
- **集中管理与系统锁定** 客户系统的各个方面将可以由中心管理员通过网络进行控制。为了维持交叉用户组受约束的、一致的以及安全的配置，通过几个简单的步骤，系统就可以被锁定。灵活性的程度可以按照 per-user(每用户)的原则由中心管理员改变，而不必改变硬件或软件。
- **应用程序灵活性的最佳方案设计** Active Platform——关键的客户与服务器 Internet 技术——在 Windows 上的完整实现，提供了配置 Web 风格的“瘦客户”应用程序和客户——服务器应用程序的灵活性，因而大大提高了效率。如果与锁定特性结合，管理员就能为每个用户精确调整所需要的客户环境，还能够按照商业需求改变这些环境。

ZAW 发表后三年半，Microsoft 在 Windows 2000 中提供了承诺的全部 ZAW。在过渡时期，Windows NT 与 95，最后是 Windows 98 客户，逐渐实现了 ZAW 特性的子集。

1.1.1 集中管理与锁定

系统策略通过永久改变 Windows NT 与 9x 用户的 HKLM 和 HKCU 注册表值实现 ZAW 的集中管理与系统锁定特性。如果决定通过简单删除来自 Netlogon 共享 Ntconfig.pol 和 Config.pol 文件的方法解除客户机上系统策略的约束，由永久注册表项施加的锁定约束仍然对用户起作用，Microsoft 称此缺陷为“注册表纹身”。必须在 Poledit.exe 中明确禁止先前允许的每一个系统策略，改变客户机的注册表项。此过程是无趣的，尤其是已经实现了一个非常有限制性的系统策略集。

说明： 组策略与系统策略利用模板(.adm)定义每一个策略并指定由策略设置修改的注册表键与值。组策略与 adm 模板类似，但是与系统策略的模板不同。系统模板将其设置保存在一个单独的.pol 文件中，组策略将其设置保存在 AD 中和两个注册表.pol 文件中，一个用于 Computer Configuration，而另一个用于 User Configuration。

组策略通过将其注册表的变化放在下列两组受保护的键中克服了“纹身”问题：

- 用于计算机的，在计算机引导时加载的 HKLM\Software\Microsoft\Windows\CurrentVersion\Policies 和 HKLM\Software\Policies\Microsoft。
- 用于用户的，在用户登录时加载的 HKCU\Software\Microsoft\Windows\CurrentVersion\Policies 和 HKCU\Software\Policies\Microsoft。

说明： 附录 A 包括 Windows 2000 所有策略的描述和注册表键与值的名。

与对系统策略的改变不同，系统策略仅在用户注册时加载，对组策略的改变按照