



Microsoft®

Microsoft®
**Windows® 2000
Server**

**Distributed
Systems
Guide**

Microsoft 著

IT Professional

北京大学出版社

<http://cbs.pku.edu.cn>

Microsoft Press

微软指定参考书

Microsoft Windows 2000 Server Distributed Systems Guide

Microsoft 著

北京大学出版社

内 容 简 介

“Microsoft Windows 2000 Server Resource Kit”丛书共由7卷和一张光盘组成，光盘中包括各种工具、附加的参考资料和本丛书的电子版。当需要补充新的信息时，我们将通过Web发布，读者可通过Web得到有关的更新内容和信息。

《Windows 2000 Server Distributed System Guide》分别从概念、理论、功能和实用的角度，对构成Windows 2000分布式系统的各种技术进行了详细的介绍和分析。本书主要围绕以下四个方面进行了深入的技术分析：Active Directory、分布式系统的安全、企业技术和桌面配置管理。

Copyright (2000) by Microsoft Corporation

Original English language edition Copyright © 2000 (year of first publication by author)

By Microsoft Corporation (author)

All rights published by arrangement with the original publisher, Microsoft Press, a division of Microsoft Corporation, Redmond, Washington, U.S.A.

北京市版权局著作权合同登记号：图字 03-2000-0288

图书在版编目(CIP)数据

Microsoft Windows 2000 Server 分布式系统指南：英文/美国微软公司(Microsoft)著。
—影印本。—北京：北京大学出版社，2000.3

(MCSE 培训教程)

ISBN 7-301-01419-8

I. M... II. 美... III. 分布式操作系统, Windows 2000-英文 IV. TP316.4

中国版本图书馆CIP数据核字(2000)第04212号

书 名：Microsoft Windows 2000 Server 分布式系统指南

责任著作者：Microsoft 著

标准书号：ISBN 7-301-01419-8/TP·84

出 版 者：北京大学出版社

地 址：北京市海淀区中关村北京大学校内 100871

网 址：<http://cbs.pku.edu.cn>

电 话：出版部 62752015 发行部 62754140 编辑室 62765127

电 子 信 箱：zwxu@mail.263.net.cn

印 刷 者：中国科学院印刷厂

发 行 者：北京大学出版社

经 销 者：新华书店

787毫米×1092毫米 16开本 106.5印张 2475千字

2000年3月第一版 2000年3月第一次印刷

定 价：348.00元

出版说明

Microsoft Windows 2000 操作系统现在已经正式推出了。微软公司的操作系统在世界计算机市场上有很大的安装率。自然,对于新推出的 Windows 2000 操作系统,也一定能够受到用户的欢迎,并得到广泛普及。

这套 Microsoft Windows 2000 影印书是属于微软的 Resource Kit 系列的,对 Windows 2000 的资源进行了详细的剖析。与此同时,我们还推出了一套 Microsoft Windows 2000 Resource Kit 系列影印书。选择这两套书出版,我们考虑到它们有一个共同点,就是都是介绍 Windows 2000 操作系统的。对于未来操作系统的主流,这套书对读者和将参加各类计算机水平考试的人来说,都是有很大参考价值的。

这两套书在实际应用中的重要性可以体现在如下几个方面:

1. IT 业在其整个信息技术生命周期内,微软的 Training Kits 和 Resource Kits 对人员的帮助占据了主导地位。

2. 大多数情况下,IT 人员使用 Resource Kits 来协助自己工作(在配置阶段占 74%,在支持阶段占 84%)。

3. 在进行的调查中,发现大多数 IT 人员认为微软系列非常有用(Training Kits 为 62%, Resource Kits 为 68%)。

4. 如果没有微软系列,IT 业的从业人员就不得不使用其他资源(包括其他技术计算机书、杂志、培训班、网站和网络技术等),而这些资源光材料费就得花费近 3000 美金,且劳动力消耗也超过了微软。在不同阶段,情况如下所示:

- 在 IT 整个周期的培训阶段,IT 人员发现在劳动力消耗上,由于有微软的 Training Kits,使他们节约了 1879 美金, Resource Kits 使他们节约了 3142 美金。
- 在评估阶段,数字也是相似的:在劳动力消耗上,微软的 Training Kits 使工作平均节约 1611 美金, Resource Kits 平均节约了 2368 美金。
- 在配置阶段, Training Kits 使每个劳动力平均节约了 5429 美金, Resource Kits 为 1339 美金。
- 在支持阶段,节约数字和配置阶段相似, Training Kits 节约了 5732 美金, Resource Kits 节约了 1754 美金。

5. 微软系列不仅在材料和劳动力消耗的节约上很有价值,在防止错误决策方面也是很有价值的。被调查的 IT 人员中,一半的人发现在防止错误决策方面,微软的 Training Kits

和 Resource Kits 为他们节约了 5000~10000 美金。

6. 被调查的 IT 人员中的 40%认为, 微软的 Training Kits 和 Resource Kits 系列中提供的信息和工具是影响他们购买或获得微软产品决定的因素。

7. 58%的 IT 人员已经使用了微软的 Training Kits 和 Resource Kits 系列去配置他们的产品, 而且几乎每个人都发现他们是最有用的产品, 在配置上给他们帮了很大的忙。

上面的这些数字虽然来自于美国, 但对于快速增长的中国 IT 业, 无疑同样有着巨大的参考价值。为什么这么说呢? 因为 Windows 2000 操作系统具有很多先进的特性, 必将成为操作系统的主流, 所以掌握它也就很必要了。同时, 作为其服务器版的 Windows 2000 Server, 功能又相对复杂。这种情况下, 借助于权威的、专业的图书, 无疑能有良好的效果。通过阅读本系列书, 可以使公司的在职人员、高级管理人员和开发人员具有良好的技能, 全面提高工作效率。

另: 本套丛书有配套光盘一张, 里面有本丛书的电子文档、工具软件等, 价格 252 元。有需要的用户可与 010-62765127 或 zwxu@mail.263.net.cn 联系。

出版者

Introduction

Welcome to the *Microsoft® Windows® 2000 Server Resource Kit Distributed Systems Guide*.

The *Microsoft® Windows® 2000 Server Resource Kit* consists of seven volumes and a single compact disc (CD) containing tools, additional reference materials, and an online version of the books. Supplements to the *Windows 2000 Server Resource Kit* will be released as new information becomes available, and updates and information will be available on the Web on an ongoing basis.

The *Distributed Systems Guide* provides a conceptual, theoretical, functional, and practical view of the various technologies that make up the Microsoft® Windows® 2000 distributed systems. This guide provides in-depth technical information that encompasses four major areas: Active Directory™, distributed security, enterprise technologies, and desktop configuration management.

Document Conventions

The following style conventions and terminology are used throughout this guide.

Element	Meaning
bold font	Characters that you type exactly as shown, including commands and switches. User interface elements are also bold.
<i>Italic font</i>	Variables for which you supply a specific value. For example, <i>Filename.ext</i> could refer to any valid file name for the case in question.
Monospace font	Code samples.
%SystemRoot%	The folder in which Windows 2000 is installed.

Reader Alert	Meaning
Tip	Alerts you to supplementary information that is not essential to the completion of the task at hand.
Note	Alerts you to supplementary information.
Important	Alerts you to supplementary information that is essential to the completion of a task.
Caution	Alerts you to possible data loss, breaches of security, or other more serious problems.
Warning	Alerts you that failure to take or avoid a specific action might result in physical harm to you or to the hardware.

Resource Kit Compact Disc

The *Windows 2000 Server Resource Kit* companion CD includes a wide variety of tools and resources to help you work more efficiently with Windows 2000.

Note The tools on the CD are designed and tested for the U.S. version of Windows 2000. Use of these programs on other versions of Windows 2000 or on versions of Microsoft® Windows NT® can cause unpredictable results.

The *Resource Kit* companion CD contains the following:

Windows 2000 Server Resource Kit Online Books An HTML Help version of the print books. Use these books to find the same detailed information about Windows 2000 as is found in the print versions. Search across all of the books to find the most pertinent information to complete the task at hand.

Windows 2000 Server Resource Kit Tools and Tools Help Over 200 software tools, tools documentation, and other resources that harness the power of Windows 2000. Use these tools to manage Active Directory™, administer security features, work with the registry, automate recurring jobs, and many other important tasks. Use Tools Help documentation to discover and learn how to use these administrative tools.

Windows 2000 Resource Kit References A set of HTML Help references:

- **Error and Event Messages Help** contains most of the error and event messages generated by Windows 2000. With each message comes a detailed explanation and a suggested user action.
- **Technical Reference to the Registry** provides detailed descriptions of Windows 2000 registry content, such as the subtrees, keys, subkeys, and entries that advanced users want to know about, including many entries that cannot be changed by using Windows 2000 tools or programming interfaces.
- **Performance Counter Reference** describes all performance objects and counters provided for use with tools in the Performance snap-in of Windows 2000. Use this reference to learn how monitoring counter values can assist you in diagnosing problems or detecting bottlenecks in your system.
- **Group Policy Reference** provides detailed descriptions of the Group Policy settings in Windows 2000. These descriptions explain the effect of enabling, disabling, or not configuring each policy, as well as explanations of how related policies interact.

Resource Kit Support Policy

The software supplied in the *Windows 2000 Server Resource Kit* is not supported. Microsoft does not guarantee the performance of the *Windows 2000 Server Resource Kit* tools, response times for answering questions, or bug fixes to the tools. However, we do provide a way for customers who purchase the *Windows 2000 Server Resource Kit* to report bugs and receive possible fixes for their issues. You can do this by sending e-mail to rkinput@microsoft.com. This e-mail address is only for *Windows 2000 Server Resource Kit* related issues. For issues relating to the Windows 2000 operating system, please refer to the support information included with your product.

Contents

Introduction	xliv
Document Conventions	xliv
Resource Kit Compact Disc	xlvi
Resource Kit Support Policy	xlvii

Part 1 Active Directory

Chapter 1 Active Directory Logical Structure	3
Active Directory Domain Hierarchy	5
Active Directory Domain Names	6
DNS Naming Conventions	7
NetBIOS Domain Names	9
Active Directory and DNS	10
DNS Hierarchy and Active Directory	10
DNS and the Internet	11
Active Directory and the Internet	12
DNS Host Names and Windows 2000 Computer Names	12
DNS Name Servers and Zones	13
Active Directory–Integrated DNS	15
Support for Dynamic Updates	18
Tree and Forest Structure	18
Tree: Implementation of a Domain Hierarchy and DNS Namespace	19
Forest: Implementation of All Trees	20
Forest Root Domain	22
Trust Relationships	23
Transitive and Nontransitive Trust	24
Direction of Trust	25
Authentication Protocols	26
Trust Path	27
Processing Authentication Referrals	28
Types of Trust Relationships	30
Trust Relationships Between Windows 2000 and Windows NT 4.0 Domains	33
Mixed-Environment Scenario	34

Active Directory Objects	35
Object Naming	36
Distinguished Name	36
Relative Distinguished Name	37
Naming Attributes	38
Object Identity and Uniqueness	39
Active Directory Name Formats	39
DNS-to-LDAP Distinguished Name Mapping	40
Logon Names	41
Domain Controllers	42
Multimaster Operations	42
Single-Master Operations	43
Global Catalog Servers	44
Global Catalog Attributes	45
Designating a Global Catalog	45
Global Catalog and Domain Logon Support	46
Search Requests and the Global Catalog	47
Organizational Units	48
Administrative Hierarchy	48
Group Policy	48
Delegation of Control	49
Object Security	49
Access Control	50
Delegation of Administration	50
Inheritance	51
Additional Resources	51

Chapter 2 Active Directory Data Storage 53

Active Directory Architecture	55
Active Directory and Windows 2000 Architecture	55
Security Subsystem Architecture	56
Directory Service Architecture	59
Directory System Agent	62
Database Layer	63
Extensible Storage Engine	63

Protocols and Interfaces to Active Directory	64
LDAP	65
ADSI	69
Active Directory Replication	70
MAPI	71
SAM	71
Data Storage	73
Data Characteristics	74
Storage Limits	75
Object Size vs. Maximum Database Record Size	75
Garbage Collection	76
Database Defragmentation	78
Growth Estimates for Active Directory Users and Organizational Units	81
Directory Database Sizing Tests	82
Organizational Units	84
Adding Attributes	84
Windows 2000 SAM Storage	86
Mixed-Mode Storage Considerations	87
SAM Structure	88
SAM Accounts on a Windows 2000 Server That Becomes a Domain Controller	88
Migration of Windows NT 4.0 SAM Accounts to Active Directory Objects	89
Data Model	91
Container Objects and Leaf Objects	91
Directory Tree	92
RootDSE	93
Extended LDAP Controls	97
Attribute Range Option	98
Directory Partitions	99
Directory Partition Subtrees	99
Forest Root Domain	101
Configuration Directory Partition	102
Schema Directory Partition	106
Domain Directory Partitions	107

Directory Data Store	111
Linked Attributes	112
Searching on Back Links	113
Group Members from External Domains	115
Phantom Records	117
Database Write Operations	117
Log-based Recovery	118
Attribute Indexing	118
Object-Based Security	119
Security Identifiers	119
Security Descriptors	120
Default Object Security	120
Installing Active Directory	121
Active Directory Configurations	123
Installation Prerequisites and Verifications	125
Verify Unique Names	126
Verify That TCP/IP Is Installed	126
Verify That DNS Client Is Configured	127
Get and Validate the DNS Domain Name	127
Get and Validate the NetBIOS Name	127
Enter Administrative Password	128
Get Credentials for the User	128
Get and Verify File Paths	129
Configure Site	129
Directory Service Configuration	130
Configuring Directory Partitions	131
Setting Services to Start Automatically	131
Setting Security	132
Creating a New Domain	135
DNS Installation and Configuration	140
Operations That Occur Following Installation	140
Removing Active Directory	141
Administrative Credentials	142
Removal from an Additional Domain Controller or the Last Domain Controller	142
Removal of an Additional Domain Controller	143
Removal of the Last Domain Controller	143
Unattended Setup for Installation or Removal of Active Directory	144

Chapter 3	Name Resolution in Active Directory	145
Locating Active Directory Servers	147	
Domain Controller Name Registration	147	
DNS Domain Name Registration	148	
NetBIOS Domain Name Registration	150	
SRV Resource Records	150	
_msdc Subdomain	151	
SRV Records Registered by Net Logon	151	
Host Records for Non-SRV-Aware Clients	155	
Other SRV Record Content	156	
Domain Controller Location Process	157	
DsGetDcName API	158	
Finding a Domain Controller in the Closest Site	161	
Active Directory Site and Subnet Objects	162	
Mapping IP Addresses to Site Names	163	
Automatic Site Coverage	164	
Cache Time-out and Closest Site	166	
Clients with No Apparent Site	167	
Types of Locators	168	
IP/DNS-Compatible Locator Process for Windows 2000 Clients	168	
Windows NT 4.0-Compatible Locator Process for Non-IP/DNS Clients	171	
Finding Information in Active Directory	174	
Resolving Names in Directory Operations	174	
Components of an LDAP Search	175	
Search Filters	176	
ObjectCategory vs. ObjectClass in a Search Filter	178	
LDAP Referrals	178	
Knowledge References	179	
Subordinate References	181	
Cross-References	181	
Creating External Cross-References	183	
Superior References	186	
Ambiguous Name Resolution	186	
Anonymous Queries	189	
Using Access Control to Enable Anonymous Access	190	
Security Precautions for Anonymous Access	192	

Global Catalog and LDAP Searches	193
Global Catalog Servers	193
Searching the Global Catalog vs. Searching the Domain	193
Searching for Deleted Objects	196
LDAP Search Clients	197
Administrative Clients	197
Windows Address Book	199
Ldp	202
Chapter 4 Active Directory Schema	203
Introduction to the Active Directory Schema	205
Location of the Schema in Active Directory	206
Finding the Schema Container	207
Subschema Subentry	209
Schema Files	209
Active Directory Schema Objects	210
<i>attributeSchema</i> Objects	210
Single-Value or Multivalue Attributes	211
Indexed Attributes	211
Attributes for <i>attributeSchema</i> Class Objects	212
<i>classSchema</i> Objects	214
Categories of Object Classes	215
Inheritance	217
System and Changeable Attribute Pairs	218
Mandatory Attributes	218
Attributes for <i>classSchema</i> Objects	220
Syntaxes	222
Object Identifiers	224
Structure and Content Rules	226
Schema Cache	228
Default Security of Active Directory Objects	229
Default Security of the Domain Directory Partition	229
Default Security of the Configuration Directory Partition	230
Default Security of the Schema Directory Partition	231
Default Security of Attributes and Classes	231

Extending the Schema	232
When to Extend the Schema	232
How to Extend the Schema	233
Installation of Schema Extensions	234
Specify the Schema-ID-GUID	235
Naming	235
Modifying the Schema	236
Schema Administrators Group	237
Schema FSMO Role	238
Order of Processing When Extending the Schema	242
Adding and Modifying Schema Objects	243
Adding an Attribute	243
Modifying an Attribute	246
Adding a Class	246
Modifying a Class	248
System Checks and Restrictions Imposed on Schema Additions and Modifications	249
Consistency Checks	249
Safety Checks	251
Deactivating Schema Objects	252
Disabling Existing Classes and Attributes	255
Effect of Deactivating a Schema Object on All Objects	256
Effects of Deactivating a Schema Object on Schema Updates	257
Issues Related to Modifying the Schema	258
Replication	258
Concurrency Control	258
Handling Invalid Object Instances	259
Methods for Extending the Schema	260
LDAP Data Interchange Format	260
Comma-Separated Value File Format	266
Using LDIFDE and CSVDE to Modify the Schema	269
Using Active Directory Service Interfaces and Visual Basic Scripts	272
Using the Active Directory Schema Console	274

Chapter 5 Service Publication in Active Directory 275**Introduction to Service Publication 277**

Types of Service Information 277

Service Objects 278

Service Bindings 278

Service Instantiation 279

Directory Infrastructure for Service Publication 280

Connection Points 281

Where to Publish 282

Computer Object 284

Organizational Unit Container Hierarchy 284

Users and Computers Containers 284

System Container 285

Publishing Services in Active Directory 286

Publishing with the RPC Name Service (RpcNs) 288

Publishing with Windows Sockets Registration and Resolution (RnR)
288**Finding and Viewing Service Information In Active Directory 289****Windows 2000 RPC Name Service and Integration with Active Directory 290**

Windows 2000 RPC Name Service Process 291

Security Considerations for All Services 293

Mutual Authentication 295

Principal Names 295

Mutual Authentication and Kerberos 296

Service Principal Names 296

Service Principal Names Syntax 297

Creating the Service Principal Name 297

Additional Resources 298**Chapter 6 Active Directory Replication 299****Active Directory Replication Model 301**

Directory Partition Replicas 301

Replication Model Benefits 302

Replication Model Components 303

Multimaster Replication 304

Store-and-Forward Replication 305

Pull Replication 306

State-based Replication 306

Replication Behavior 307

Active Directory Updates	309
Originating Updates: Initiating Changes	309
Tracking Updates	310
Deciding What Changes to Replicate: Update Sequence Numbers	311
Resolving Conflicts: Stamps	314
Originating Add	315
Originating Modify	315
Originating Move	316
Originating Delete	316
Tracking Object Creation, Replication, and Change	317
Propagation Dampening	319
Multimaster Conflict Resolution Policy	320
Replication Topology	321
Topology Concepts and Components	322
Topology-related Components	322
Sites Container Hierarchy in Active Directory	325
Sites and Replication	326
Replication Efficiency	327
Site Design with Replication in Mind	327
Subnet-to-Site Mapping	328
When to Define a New Site	329
Default Site	330
Server and Site Connections	330
Server Objects	331
Server Connections	332
Site Links	334
Bridgehead Servers	335
Replication Transports	335
Synchronous vs. Asynchronous Communication	336
Transport for Replication Within a Site	336
Transports for Replication Between Sites	338
Replication Packet Size	340