

Windows Server 2003

活动目录

实战指南

刘晓辉 王淑江 等 编著



- 活动目录整体规划
- 域控制器具体部署
- 用户权限全面管理
- 策略认证深入应用
- 状态性能远程监控
- 目录故障诊断排除

 人民邮电出版社
POSTS & TELECOM PRESS

Windows Server 2003

活动目录

Windows Server 2003 活动目录

作者：[美] 比尔·盖特



- 活动目录概述
- 活动目录架构
- 活动目录部署
- 活动目录管理
- 活动目录安全
- 活动目录性能

清华大学出版社

Windows Server 2003

活动目录实战指南

刘晓辉 王淑江 等编著

人民邮电出版社
北 京

图书在版编目 (CIP) 数据

Windows Server 2003 活动目录实战指南 / 刘晓辉等编著.

—北京: 人民邮电出版社, 2007.3

ISBN 978-7-115-15706-5

I. W... II. 刘... III. 服务器—操作系统 (软件), Windows Server 2003—指南
IV. TP316.86-62

中国版本图书馆 CIP 数据核字 (2006) 第 161758 号

内 容 提 要

本书从活动目录的实际应用入手, 引导读者理解活动目录的原理与操作, 掌握活动目录的设计与实施, 以满足网络服务和管理的需要。书中内容涉及活动目录林和域的规划与设计, 组织单元、用户和用户组的管理, 域控制器的管理与维护, 组策略、动态 DNS、身份认证、权限管理等网络目录应用, 以及活动目录的性能监控与故障排除。

本书内容全面、语言简练、深入浅出、图文并茂、贴近实战, 是一本不可多得的活动目录技术参考书。

本书适用于技术支持人员、系统管理人员、网络管理人员、MCSE 应试人员, 以及对计算机系统维护和网络管理感兴趣的计算机爱好者。

Windows Server 2003 活动目录实战指南

- ◆ 编 著 刘晓辉 王淑江 等
责任编辑 陈 昇
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
人民邮电出版社河北印刷厂印刷
新华书店总店北京发行所经销
- ◆ 开本: 787 × 1092 1/16
印张: 47.5
字数: 1 509 千字
印数: 1—5 000 册
- 2007 年 3 月第 1 版
2007 年 3 月河北第 1 次印刷

ISBN 978-7-115-15706-5/TP

定价: 78.00 元

读者服务热线: (010)67132705 印装质量热线: (010)67129223

前 言

随着网络资源的不断丰富和网络应用的不断深入,对用户安全和访问权限的要求也就越来越高,对用户实现自动化管理的需要也就越来越迫切。在这种情况下,安装一台或多台域控制器、创建活动目录,实现网络用户访问权限、身份认证、用户界面的统一管理,就成为一种必要。

活动目录作为网络资源的集合,不仅容纳了网络内所有的共享资源(共享文件夹、共享打印机等),而且也容纳了网络内的所有用户和用户组。因此,借助活动目录,不仅可以让用户迅速、容易地找到所需要的数据,而且可以轻松实现对用户访问权限的限制与管理。

作为定制用户桌面与安全的组策略,与活动目录紧密联系在一起。借助组策略,可以有效地实现对网络客户的控制与管理,从而实现对用户访问权限的控制,并实现软件分发、系统更新、远程安装等管理任务,最大限度地保证客户端、乃至整个网络的安全。此外,许多网络服务(如动态 DNS 服务、DFS 服务等)和网络安全认证(如 IIS 认证、VPN 认证、IEEE802.1x 认证等)也都依赖于活动目录。

由此可见,活动目录在网络中拥有不可替代的重要位置。作为一本对活动目录的配置和应用进行全面阐述图书,相信一定会得到广大系统管理员的认同和欢迎。

作为一个系统管理员,在网络搭建完成并实现一些基本的网络服务之后,接下来要考虑的就是如何保障网络资源的访问安全,如何保证数据的存储安全;如何避免对网络的滥用;如何实现系统的快速维护,以及操作系统和应用软件的快速分发。尽管可以采取的措施非常多,但是,所有的技术手段都离不开活动目录的支持。因此,只有安装并配置了活动目录,才能很好地实现这一切。

既然活动目录如此重要,而许多系统管理员对活动目录又知之甚少,那么,我们现在适时推出这样一本专门的图书,应当说与网络的发展步伐是合拍的,与网络发展需求是吻合的,也必然会得到广大系统管理员的认同。本书从实际应用的角度出发,全面深入地探讨了活动目录管理的方方面面,包括了规划设计、对象管理、配置维护、认证应用、故障排除、性能监控等所有关于活动目录的理论与技术。

本书由刘晓辉、王淑江编著,田俊乐、王春海、李海宁、陈志成、韩文智、赵卫东、刘淑梅、李文俊、杨伏龙、许广博、白晓明、肖丽芳等也参与了部分章节的编写工作。笔者长期从事系统维护和网络管理工作,具有一定的理论水平和丰富的实践经验,迄今为止,已经出版了 50 余部计算机类图书,均以易读、易学、实用的特点,受到众多读者的一致好评。本书是作者的又一呕心沥血之作,希望能对大家的系统维护和网络管理工作有所帮助。由于笔者水平所限,书中难免存在一些错误与不足,希望读者不吝赐教。另外,如果读者对本书有何疑问或需要获得技术支持,请发 E-mail 至 hslxh@163.com。

编 者
2007.1

目 录

第 1 章 活动目录概述	1
1.1 活动目录概述	1
1.1.1 活动目录的重要意义	1
1.1.2 活动目录对象	2
1.1.3 活动目录组件	6
1.1.4 逻辑结构	7
1.1.5 物理结构	8
1.2 理解活动目录概念	9
1.2.1 全局目录 (GC)	9
1.2.2 复制	10
1.2.3 信任关系	10
1.2.4 DNS 名称空间	11
1.2.5 名称服务器	13
1.2.6 命名规范	14
1.2.7 域控制器	14
1.3 活动目录的新特性	15
1.3.1 活动目录的优点	15
1.3.2 活动目录新特性和改进	15
第 2 章 DNS 与活动目录	18
2.1 DNS 概述	18
2.1.1 DNS 简介	18
2.1.2 名称空间	19
2.1.3 DNS 和活动目录的区别	20
2.1.4 DNS 与活动目录集成	21
2.2 规划 DNS	21
2.2.1 服务规划	21
2.2.2 逻辑规划	23
2.2.3 服务器硬件规划	24
2.2.4 安全规划	27
2.3 DNS 安装	29
2.3.1 IP 地址设置	29
2.3.2 向导方式安装	30
2.3.3 组件方式安装	33
2.4 AD 集成区域第一台 DNS 服务器	33
2.4.1 目录集成区域的优点	34

2.4.2 主要 DNS 服务器	34
2.4.3 AD 集成区域的 DNS 服务器	38
2.4.4 AD 集成区域 DNS 验证	46
2.5 AD 集成区域第二台 DNS 服务器	48
第 3 章 活动目录部署	52
3.1 Active Directory 评估	52
3.1.1 Active Directory 架构环境	52
3.1.2 Active Directory Sizer 工具评估应用环境	52
3.2 Active Directory 规划	58
3.2.1 案例说明	59
3.2.2 AD 名称空间	60
3.2.3 域林	61
3.3 Active Directory 部署	65
3.3.1 安装第一个企业根域控制器域名 book.com	65
3.3.2 安装辅助域控制器	71
3.3.3 安装根域 book.com 下的第一个子域 bj.book.com	74
3.3.4 安装根域 book.com 下的第 2 个域树 Pen.com	78
3.3.5 添加域林的第 1 个子域 bj.book.com 的成员服务器 SR1	81
3.3.6 创建域林	83
3.3.7 删除 Active Directory	89
3.3.8 重命名 Active Directory	92
第 4 章 活动目录操作主机	101
4.1 操作主机概述	101
4.1.1 操作主机	101
4.1.2 架构主机	102
4.1.3 域命名主机	102
4.1.4 PDC 仿真器	102
4.1.5 RID 主机	103
4.1.6 基础结构主机	103
4.2 查看操作主机角色	103
4.2.1 GUI 模式	104
4.2.2 命令行模式	107
4.2.3 脚本方式	108
4.3 操作主机规划	110
4.3.1 环境描述	110
4.3.2 FSMO 规划	111
4.4 操作主机转移	112
4.4.1 角色转移	112
4.4.2 GUI 模式转移操作主机角色	113
4.4.3 命令行模式	119
4.5 占用操作主机角色	122
4.5.1 故障状况	122
4.5.2 占用操作主机角色	123

第 5 章 活动目录的站点	127
5.1 站点概述	127
5.1.1 站点任务	127
5.1.2 独立站点	128
5.1.3 多个站点	128
5.1.4 站点管理	129
5.1.5 KCC	129
5.1.6 默认站点	130
5.2 站点规划	130
5.2.1 案例介绍	130
5.2.2 站点规划	131
5.3 Active Directory 站点配置	132
5.3.1 创建站点	132
5.3.2 创建子网并连接站点	133
5.3.3 创建站点链接	134
5.3.4 移动服务器	135
5.3.5 给站点授权计算机	136
5.3.6 站点委派控制	137
5.3.7 站点链接搭桥	138
5.3.8 KCC 手工检测	141
第 6 章 活动目录复制	142
6.1 复制概述	142
6.1.1 复制简介	142
6.1.2 复制类型	143
6.1.3 复制机制	144
6.1.4 复制方式	146
6.1.5 复制内容	148
6.2 复制拓扑	149
6.3 复制规划	155
6.4 管理复制	156
6.4.1 配置站点链接	156
6.4.2 站点链接开销	156
6.4.3 复制频率	156
6.4.4 设置站点链接可用性	157
6.4.5 配置站点链接桥	158
6.4.6 配置首选桥头服务器	158
第 7 章 活动目录信任	160
7.1 信任概述	160
7.1.1 信任	160
7.1.2 信任类型	160
7.1.3 信任方向	163
7.1.4 信任传递性	165

7.1.5 新的信任类型——林信任	166
7.2 信任的创建时间	167
7.2.1 何时创建外部信任	168
7.2.2 何时创建快捷信任	168
7.2.3 何时创建领域信任	168
7.2.4 何时创建林信任	168
7.3 创建信任实例	169
7.3.1 创建快捷信任	169
7.3.2 创建外部信任	172
7.3.3 创建林根信任	178
7.3.4 删除信任	179
7.3.5 验证信任	180
第8章 活动目录功能级别	182
8.1 功能级别	182
8.1.1 域功能	182
8.1.2 域功能提升	183
8.1.3 域功能级别评估	183
8.1.4 域林功能	184
8.2 提升功能级别	184
8.2.1 提升域功能级别	185
8.2.2 提升林功能级别	187
第9章 活动目录全局编录服务器	192
9.1 全局编录服务器概述	192
9.2 查看全局编录服务器	193
9.2.1 GUI方式	193
9.2.2 脚本方式	194
9.2.3 命令行方式	195
9.3 全局编录服务器规划	195
9.3.1 全局编录服务器规划原则	196
9.3.2 案例规划	196
9.4 全局编录服务器应用	197
9.4.1 域控制器提升为全局编录服务器	197
9.4.2 验证全局编录服务器的提升	198
9.4.3 验证全局编录服务器正常工作	200
9.4.4 删除全局编录服务器	203
第10章 活动目录委派	206
10.1 委派概述	206
10.1.1 组织单位	206
10.1.2 管理目标	207
10.2 委派规划	208
10.3 委派应用	209
10.3.1 创建组织单位、组、用户	210

10.3.2	创建委派任务	217
10.3.3	创建管理控制台	219
10.3.4	创建管理任务	225
10.3.5	禁止权限继承	229
10.4	受限委派	231
10.4.1	创建委派选项卡	232
10.4.2	配置委派	234
10.4.3	配置受限委派	238
第 11 章	活动目录的组织单位	243
11.1	组织单位概述	243
11.1.1	组织单位模型	243
11.1.2	组织单位和组的区别	243
11.1.3	群组原则	244
11.2	组织单位规划	244
11.2.1	规划组织单位原则	244
11.2.2	规划组织单位分层结构	245
11.3	组织单位应用	248
11.3.1	创建组织单位	248
11.3.2	移动组织单位	249
11.3.3	更改组织单位名称	251
11.3.4	删除组织单位	253
11.3.5	查找组织单位	254
11.3.6	组织单位新增用户	256
11.3.7	组织单位新增计算机	258
11.3.8	组织单位新增组	260
11.3.9	移动组织单位的成员	261
11.3.10	删除组织单位的成员	262
11.3.11	组织单位的委派	263
11.3.12	取消组织单位的权限继承	263
第 12 章	活动目录的用户	266
12.1	用户概述	266
12.1.1	用户账户简介	266
12.1.2	用户命名惯例	267
12.1.3	用户密码要求	267
12.2	创建用户	267
12.2.1	默认用户	268
12.2.2	UPN 后缀	268
12.2.3	创建域用户账户	270
12.2.4	创建企业系统管理员	272
12.2.5	查看用户属性	274
12.2.6	其他用户属性	275
12.2.7	创建大量用户	285
12.2.8	将用户添加到本地管理员组	291

12.3 管理用户	293
12.3.1 添加到组	293
12.3.2 启用、禁用账户	295
12.3.3 移动	296
12.3.4 重设密码	297
12.3.5 删除	299
12.3.6 重命名	300
12.4 用户权限和权力	301
12.4.1 用户权限	301
12.4.2 用户权力	303
12.5 用户配置文件	307
12.5.1 用户配置文件概述	307
12.5.2 漫游用户配置文件	310
12.5.3 用户配置文件设置	312
12.5.4 强制使用相同的配置文件	316
12.6 用户主目录	323
12.6.1 创建共享文件夹	323
12.6.2 指派用户主目录	324
第 13 章 活动目录的组	327
13.1 组概述	327
13.1.1 组类型	327
13.1.2 组功能	328
13.1.3 默认组	331
13.1.4 嵌套组	333
13.2 组规划	335
13.2.1 组设计原则	335
13.2.2 组规划——AGDLP 原则	336
13.3 组应用实例	337
13.3.1 创建全局安全组	337
13.3.2 移动用户到“全局组”	339
13.3.3 创建“本地域组”	341
13.3.4 “全局组”加入到“本地域组”	342
13.3.5 设置“本地域组”访问文件夹权限	343
第 14 章 活动目录的组策略	347
14.1 组策略概述	347
14.1.1 组策略的功能	347
14.1.2 组策略的组件	348
14.1.3 组策略的层次结构	349
14.1.4 计算机和用户策略的配置	352
14.2 组策略继承、委派	353
14.2.1 组策略的继承	353
14.2.2 组策略的委派	355
14.3 组策略管理控制台	360

14.3.1	GPMC 概述	360
14.3.2	GPMC 初始安装	360
14.3.3	管理组策略对象	368
14.3.4	GPO 备份、还原、复制以及导入	374
14.3.5	组策略建模	379
14.3.6	策略结果集	381
14.4	组策略综合应用	383
14.4.1	UNIX 终端仿真概述	383
14.4.2	部署环境	384
14.4.3	策略部署	385
第 15 章	活动目录与网络资源	411
15.1	发布资源	411
15.1.1	访问控制权限	411
15.1.2	发布共享文件夹	411
15.1.3	发布分布式文件系统	414
15.2	文件夹重定向	417
15.2.1	文件夹重定向概述	418
15.2.2	应用实例: 文件夹重定向	420
15.2.3	重定向文件夹测试	429
15.3	应用程序部署	431
15.3.1	软件部署策略概述	431
15.3.2	实例 1: 使用 MSI 文件部署 Office 2003	433
15.3.3	实例 2: 使用 ZAP 文件部署 HotFix	445
15.3.4	实例 3: 使用开机、关机脚本部署 HotFix	449
第 16 章	活动目录 SYSVOL 共享	453
16.1	SYSVOL 概述	453
16.1.1	SYSVOL 简介	453
16.1.2	SYSVOL 内容	453
16.1.3	SYSVOL 管理	454
16.2	SYSVOL 应用实例	455
16.2.1	SYSVOL 重定向	455
16.2.2	更改 SYSVOL 存储空间的大小	464
第 17 章	身份认证与活动目录	466
17.1	802.1x 认证与活动目录	466
17.1.1	IEEE 802.1x 身份认证概述	466
17.1.2	802.1x 认证特点	466
17.1.3	IEEE 802.1x 与 IAS	467
17.2	IIS 认证与活动目录	467
17.2.1	IIS 自身安全机制	468
17.2.2	Web 服务器身份认证	469
17.2.3	FTP 服务器身份认证	478
17.3	SMTP 与活动目录	479

17.3.1 设置身份验证方法	479
17.3.2 收件人策略	481
17.4 访问权限与活动目录	483
17.4.1 账户审核实战	483
17.4.2 限制用户登录到的计算机	485
17.4.3 委派用户权限	486
第 18 章 活动目录性能管理	492
18.1 活动目录性能监视工具	492
18.1.1 性能监视工具	492
18.1.2 事件查看器控制台	493
18.1.3 性能控制台	498
18.1.4 系统监视器	499
18.1.5 性能日志和警报	501
18.2 监视对共享文件夹的访问	505
18.2.1 监视网络资源使用	506
18.2.2 监视共享文件夹	506
18.2.3 监视打开的文件	507
18.2.4 发送控制台消息	508
第 19 章 活动目录的管理	510
19.1 活动目录管理任务	510
19.1.1 更改组成员身份	510
19.1.2 管理目录复制	510
19.1.3 创建用户和组账户	511
19.1.4 部署和升级软件包	511
19.1.5 重设用户密码	511
19.1.6 管理信任	511
19.1.7 管理全局编录	511
19.1.8 管理 FSMO	512
19.1.9 管理站点	512
19.2 活动目录管理方式	512
19.2.1 使用运行方式	512
19.2.2 使用保存的查询	517
19.2.3 MMC 管理 Active Directory	521
19.2.4 命令行管理 Active Directory	521
19.2.5 查找目录信息	522
19.3 MMC 管理控制台	524
19.3.1 MMC 控制台	524
19.3.2 管理单元	524
19.3.3 控制台选项	525
19.3.4 使用 MMC 控制台	525
19.4 Active Directory 对象	532
19.4.1 默认的 Active Directory 对象	533
19.4.2 查找活动目录对象	536

19.4.3 移动活动目录对象	538
19.4.4 站点间移动域控制器	540
19.5 Active Directory 权限管理	541
19.5.1 安全描述符	541
19.5.2 有效权限计算器	544
19.5.3 访问控制继承	546
第 20 章 管理活动目录数据库	550
20.1 Active Directory 备份和恢复	550
20.1.1 活动目录状态信息	550
20.1.2 备份 Active Directory 数据库	551
20.1.3 还原 Active Directory 数据库	555
20.2 自动备份 Active Directory 数据库	558
20.3 重定向 Active Directory 数据库	564
20.4 离线整理 Active Directory 数据库	567
20.5 修复 Active Directory 数据库	569
20.6 Active Directory 重命名	571
20.7 Active Directory 升域、降域	571
第 21 章 活动目录常见故障	572
21.1 域控制器故障	572
21.1.1 故障描述	572
21.1.2 当主域控制器出现故障, 但主域控制器仍然可用	573
21.1.3 主域控制器已经彻底损坏并且不能恢复时, 整个网络不能正常使用	580
21.2 误删用户、组或者其他对象	584
21.3 恢复任意时间域控制器备份	586
第 22 章 登录域控制器	589
22.1 登录域控制器	589
22.2 脱离域控制器	594
第 23 章 活动目录管理工具	598
23.1 Active Directory 管理工具	598
23.1.1 提升域控制器——Dcpromo	598
23.1.2 查询活动目录——Dsquery	599
23.1.3 活动目录数据库维护——Ntdsutil	611
23.1.4 显示目录对象属性——Dsget	623
23.1.5 域和林准备——Adprep	634
23.1.6 目录对象添加工具——Dsadd	635
23.1.7 修改目录对象——Dsmod	642
23.1.8 删除目录对象——Dsrm	658
23.1.9 计算机账户信任关系——Netdom	660
23.1.10 域控制器诊断工具——Dcdiag	677
23.1.11 对象模板权限工具——Dscls	680
23.1.12 目录复制工具——Repadmin	685

23.1.13	目录服务检测工具——Dsataat	688
23.1.14	目录对象处理工具——Ldifde	691
23.1.15	域信息处理高级工具——Nltest.exe	696
23.1.16	诊断活动目录对象的许可权工具——Acldiag	702
23.1.17	域间组件移动工具——Movetree	705
23.1.18	安全组件检测工具——Sdcheck	706
23.1.19	复制监视工具——Replmon	708
23.1.20	活动目录对象编辑器——Adsiedit	712
23.2	用户与组的管理	714
23.2.1	用户账户数据库管理——Net accounts	714
23.2.2	计算机账户管理——Net Computer	716
23.2.3	用户账户管理——Net user	717
23.2.4	全局组管理——Net group	719
23.2.5	本地组管理——Net localgroup	720
23.2.6	身份识别工具——Whoami	722
23.2.7	用户信息迁移工具——USMT	724
23.2.8	登录用户权限设置工具——Ntrights	727
23.2.9	组成员查看工具——Ifmember	728
23.2.10	用户锁定状态查看工具——Lockoutstatus	729
23.3	组策略工具	731
23.3.1	检查域控制器上组策略对象——GpoTool	731
23.3.2	组策略结果检测工具——GpResult	733
23.3.3	组策略刷新工具——Gpupdate	736
23.3.4	组策略管理控制台——GPMC	738
23.3.5	组策略监视器——Winpolicies	741

第 1 章 活动目录概述

活动目录 (Active Directory) 是 Windows 2000 Server 和 Windows Server 2003 系统中的目录服务。Active Directory 是一种网络服务, 它标识网络上的所有资源, 信息可以分散在多台不同的计算机上, 保证快速访问和容错; 同时, 无论用户从何处访问或信息处在何处, 它对用户都提供统一的视图。活动目录不仅集成了关键服务和关键应用, 还集成了当今关键的数据访问。

1.1 活动目录概述

活动目录 (Active Directory) 是指存储网络资源信息的目录, 以及让这些信息可供网络用户使用的服务。网络中所有的资源, 包括用户账户、文件数据、打印机、服务器、数据库、组、计算机和安全策略等, 都可以存放于活动目录中, 从而使用户的检索、使用和管理变得更加简单和方便。

1.1.1 活动目录的重要意义

电话簿中记录着亲朋好友的姓名、电话、地址、生日等信息, 可以很容易地从中找到自己想要的信息, 这就是电话目录。Windows 资源管理器中记录着文件的文件名、大小、创建和修改日期、存储位置等数据, 便于用户迅速查找自己所需要的文件, 这就是文件目录。也就是说, 目录服务所提供的功能, 就是让用户很容易地在目录内寻找所需要的数据。例如, 114 查号台是一种目录服务, 百度 (Baidu) 网站所提供的搜索功能也是一种目录服务。在 Windows Server 2003 域内提供目录服务的组件就是活动目录, 它负责目录数据库的保存、新建、删除、修改与查询等服务。

活动目录的意义在于以下几方面。

- 简化管理。谈到活动目录就不能不说起域, 域是指网络服务器和其他计算机的一种逻辑分组, 凡是在共享域逻辑范围内的用户都使用公共的安全机制和用户账户信息, 每个使用者在域中只拥有一个账户, 每次登录的是整个域。

活动目录用于将域中的资源分层次地组织在一起。每个域都包含一个或多个域控制器。域控制器是一台运行 Windows 2000 Server 或 Windows Server 2003 的计算机, 它存储域目录的一份完整的副本。为了简化管理, 域中的所有域控制器都是对等的。可以在任意一台域控制器上进行修改, 更新的内容将被复制到该域中所有其他的域控制器。活动目录为管理网络上的所有资源提供一个单一入口, 从而进一步简化了管理。因为活动目录提供一个单一的入口来登录所有网络资源, 所以管理员可以登录任意一台计算机并管理网络中任何计算机上的对象。

- 提升网络安全性。安全性通过登录身份验证及目录对象的访问控制集成在活动目录之中。通过单击网络登录, 管理员可以管理分散在网络各处的目录数据和组织单位, 经过授权的网络用户可以访问网络任意位置的资源。基于策略的管理则简化了网络的管理, 即便是那些最复杂的网络也是如此。

活动目录通过对象访问控制列表及用户凭据保护其存储的用户账户和组信息, 因为活动目录不但可以保存用户凭据, 还可以保存访问控制信息, 所以登录到网络上的用户既能够获得身份验证, 也可以获得访问系统资源所需的权限。例如, 在用户登录到网络上的时候, 安全系统首先会利用存储在活动目录中的信息验证用户的身份, 然后, 在用户试图访问网络服务的时候, 系统会检查在服务的自由访问控制列表 (DACL) 中所定义的属性。

因为活动目录允许管理员创建组账户, 管理员可以更加有效地管理系统的安全性。例如, 通过调整文件的属性, 管理员能够允许某个组中的所有用户读取该文件。通过这种办法, 系统将根据用户组的成员身份控制其对活动目录中对象的访问操作。

- 具有很强的可扩展性。Windows Server 2003 的活动目录具有很强的可扩展性, 管理员可以在计划中增加新的对象类, 或者给现有的对象类增加新的属性。计划包括可以存储在目录中的每个对象类的定义和属性。例如, 在电子商务上可以给每个用户对象增加一个购物授权属性, 然后存储每个用户购买权限作为用户账户的一部分。

- 具有很强的可伸缩性。活动目录可包含在一个或多个域中, 每个域可以有一个或多个域控制器, 以便用户可以调整目录的规模以满足任何网络的需要。多个域可组成为域树, 多个域树又可组成为树林, 活动目录也就随着域的伸缩而伸缩, 较好地适应了单位网络的变化。目录将其架构和配置信息分发给目录中所有的域控制器, 该信息存储在域的第一个域控制器中, 并且复制到域中任何其他域控制器中。当该目录配置为单个域时, 添加域控制器将改变目录的规模, 而不影响其他域的管理开销。将域添加到目录使用户可以针对不同策略环境划分目录, 并调整目录的规模以容纳大量的资源和对象。

- 智能的信息复制能力。信息复制为目录提供了信息可用性、容错、负载均衡和性能优势, 活动目录使用多主机复制, 允许用户在任何域控制器上同步更新目录。多主机模式具有更大容错的优点, 因为使用多域控制器时, 即使任何单独的域控制器停止工作, 也可继续复制。由于进行了多主机复制, 它们将更新目录的单个副本, 在域控制器上创建或修改目录信息后, 新创建或更改的信息将发送到域中的所有其他域控制器中, 所以其目录信息是最新的。域控制器需要最新的目录信息, 但是要做到高效率, 必须把自身的更新限制在只有新建或更改目录信息的时候, 以免在网络高峰期进行同步而影响网络速度。在域控制器之间不加选择地交换目录信息能够迅速搞垮任何网络。通过活动目录就能达到只复制更改的目录信息, 而不至于大量增加域控制器的负荷。

- 与 DNS 集成紧密。活动目录使用域名系统 (DNS) 来为服务器目录命名, DNS 是将更容易理解的主机名转换为 IP 地址的 Internet 标准服务, 利于在 TCP/IP 网络中计算机之间的相互识别和通信。DNS 的域名基于 DNS 分层命名结构, 这是一种倒置的树状结构, 在单个根域下面可以是父域和子域 (分支和叶子)。

- 与其他目录服务具有互操作性。由于活动目录是基于标准的目录访问协议, 许多应用程序界面 (API) 都允许开发者进入这些协议, 例如活动目录服务界面 (ADSI)、轻型目录访问协议 (LDAP) 第 3 版和名称服务提供程序接口 (NSPI), 因此它可以和使用这些协议的其他目录服务相互操作。LDAP 是用于在活动目录中查询和检索信息的目录访问协议。因为它是一种工业标准服务协议, 所以可使用 LDAP 开发程序与同时支持 LDAP 的其他目录服务共享活动目录信息。活动目录支持 Microsoft Exchange 4.0 和 5.x 客户程序所用的 NSPI 协议, 以提供与 Exchange 目录的兼容性。

- 灵活的信息查询。加入活动目录管理的任何用户均可使用“开始”菜单、“网上邻居”或“活动目录用户和计算机”上的“搜索”命令, 通过对象属性快速查找网络上的对象。例如可以通过名字、姓氏、电子邮件名、办公室位置或用户账户的其他属性来查找用户等。

1.1.2 活动目录对象

所谓的 Active Directory 对象就是指域控制器中包含相同属性的实体组成的集合, 例如计算机、用户、打印机等。属性就是用来描述目录对象可以标识的数据, 例如一个用户的属性可能是用户姓名和电子邮件地址等。安装活动目录后依次单击“开始”→“管理工具”→“Active Directory 用户和计算机”, 这里显示的都是活动目录的对象。

1. 默认容器对象

在安装活动目录过程中就已经自动创建了一些默认的容器 (Container) 对象, 这些容器对象中都包