

技术
实战指南

Windows
Server 2008

2000分钟
多媒体视频讲解

Windows Server 2008

刘晓辉 李利军 编著

活动目录应用实战指南

全新技术
案例详解
视频教学

从实际应用出发，以案例详解活动目录的安装部署、配置管理与深入应用
涵盖域组织架构规划、活动目录与访问安全数据库的备份与恢复，以及活
动目录的监控与故障排除等内容



清华大学出版社

200分钟
多媒体视频讲解

Windows Server 2008

刘晓辉 李利军 编著

活动目录应用实战指南

清华大学出版社
北 京

内 容 简 介

本书从实际应用出发,系统地介绍了 Windows Server 2008 活动目录(AD DS)的安装部署、配置管理,以及深入应用,涉及域组织架构规划、活动目录与访问安全数据库的备份与恢复,以及活动目录的监控与故障排除等内容,全书共 19 章,前十八章主要介绍 AD DS 的各种应用方法和使用技巧,并列举了大量的部署实例,第 19 章是对 Windows Server 2008 中推出的活动目录的新技术的集中介绍,便于读者与之前的 Server 操作系统进行比较。

本书重在应用,突出实战技能的培养,借助案例教学和配套多媒体教学光盘,读者可以很轻松地掌握活动目录的内容。适合具有一定网络知识水平的读者、在职网络和系统管理员,以及所有准备从事网络/系统管理的技术爱好者,可作为企事业单位网络技术部门人员的参考用书,同时也可作为培训机构的教学用书。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

Windows Server 2008 活动目录应用实战指南/刘晓辉,李利军编著.

—北京:清华大学出版社,2010.1

ISBN 978-7-302-21218-8

I.W… II. ①刘… ②李… III. 服务器—操作系统(软件), Windows Server 2008 IV. TP316.86

中国版本图书馆 CIP 数据核字(2009)第 174323 号

责任编辑:夏非彼 卢 亮

责任校对:闫秀华

责任印制:王秀菊

出版发行:清华大学出版社

地 址:北京清华大学学研大厦 A 座

<http://www.tup.com.cn>

邮 编:100084

社 总 机:010-62770175

邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者:清华大学印刷厂

装 订 者:北京国马印刷厂

经 销:全国新华书店

开 本:190×260 印 张:29.75 插 页:2 字 数:692 千字

附光盘 1 张

版 次:2010 年 1 月第 1 版 印 次:2010 年 1 月第 1 次印刷

印 数:1~4000

定 价:59.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。联系电话:(010)62770177 转 3103 产品编号:031618-01

前言

活动目录(Active Directory)在 Windows Server 2008 中被称为 AD DS(Active Directory Domain Services, 活动目录域服务)。Windows Server 2008 提供了 3 种新的域服务模式, 分别为完全图形模式的 AD DS 域服务、只能“读取”的只读型 AD DS 域服务以及 ServerCore 模式的命令行 AD DS 域服务。不同的域服务模式, 对应的应用环境不同。只读型 AD DS 域服务适用于企业的分支机构或者拥有低速传输媒介的环境中; ServerCore 模式 AD DS 域服务适用于具备大量用户的企业, 以及对效率及稳定性要求较高的环境中。

本书以 Windows Server 2008 提供的基础服务入手, 完全以实际应用为基础, 手把手地讲解如何使用 Active Directory 服务实现管理, 借以引导读者独立完成在不同的应用中的用户管理。全书共 19 章, 从 Windows Server 2008 安装开始介绍直至服务器各项具体部署, 全面实现基于 Active Directory 的各种应用。

第 1 章 部署 AD DS 域服务: 介绍在搭建的新网络环境中如何部署 AD DS 域服务, 以及使用 AD DS 域服务如何部署额外域控制器。

第 2 章 升级域控制器: 介绍从 Windows Server 2003 的 Active Directory 环境中如何升级至 Windows Server 2008 的 AD DS 域服务, 以及升级成功后对 Windows Server 2003 域控制器的处理。

第 3 章 域迁移: 介绍从 Windows Server 2003 的 Active Directory 环境中, 迁移至 Windows Server 2008 的 AD DS 域服务, 适用于将一个域中的用户或者其他信息迁移到一个新的域。

第 4 章 管理计算机帐户: 介绍计算机帐户在实际工作中的作用, 用户加域的权限、升/降域的方法, 以及常见的管理任务。

第 5 章 管理组 and 用户: 介绍组的分类以及组的作用域, 在本章将可学习到如何进行对用户帐户的任务管理, 包括用户配置文件、用户权限以及用户权利的应用方法。

第 6 章 组织单位管理: 介绍组织单位的概念、如何规划以及其管理任务实现。

第 7 章 部署子域与域树: 介绍子域与域树的基础知识, 信任关系以及部署情况。

第 8 章 部署只读域控制器: 介绍为分支机构部署只读域控制器, 在类似的环境中, 可以取代“子域”降低分支机构的管理难度。

第 9 章 权限委派管理: 介绍客户端管理控制台的部署, 以及委派方法。

第 10 章 组策略管理: 介绍组策略管理工具、配置以及组策略的相应管理设置。

- 第 11 章 AGPM 高级组策略管理：**介绍 AGPM 高级组策略的基础知识，以及如何部署 AGPM 服务器和客户端组件。
- 第 12 章 部署首选项：**介绍组策略管理的新功能，该功能和组策略的不同是用户应用首选项策略后，可以继续配置策略，客户端计算机用户对发布的策略具备可控权限。
- 第 13 章 终端服务桌面应用：**介绍终端服务以及远程桌面应用部署方法。
- 第 14 章 用户隔离：**介绍使用“网络策略和访问”角色部署增强用户安全验证的方法，此角色将和 DHCP 角色结合使用。
- 第 15 章 管理 FSMO：**概述了 ADDS 特殊服务，FSMO 角色及其部署，并介绍了如何识别和维护角色支持器。
- 第 16 章 活动目录数据库与备份：**介绍 Active Directory 数据库的管理方法以及对数据库的备份与恢复。
- 第 17 章 监控系统和活动目录：**介绍使用 Spotlight 监控软件对 Windows 系统性能和活动目录进行监控。
- 第 18 章 活动目录故障诊断与排除：**介绍 Active Directory 故障诊断访方法，包括排除基础服务的故障以及排除活动目录的故障。
- 第 19 章 活动目录的新技术：**为方便读者与 Windows Server 2003 比较，本章集中介绍 Windows Server 2008 中推出的活动目录的新技术。

本书由刘晓辉、李利军编著，李书满、吴琪菊、余素芬、吴海燕、赵敏捷、费一峰、毛向城、朱志明、朱春英、彭文芳、陈飞、傅维佳、张建、李海宁、陈志成、田俊乐、刘国增、王延杰、刘红等也参与了本书部分章节的编写工作。虽然在写作过程中作者已经竭力注意，但疏漏和不足之处恐难避免，敬请广大读者批评指正

编 者
2010 年 01 月

目 录

第 1 章 部署 AD DS 域服务	1
1.1 安装 Windows Server 2008	2
1.1.1 硬件需求	2
1.1.2 安装方式	3
1.1.3 全新安装 Windows Server 2008	4
1.2 AD DS 域服务基础知识	7
1.2.1 设置网络参数	7
1.2.2 服务器类型	10
1.2.3 AD DS 服务器角色	10
1.2.4 AD DS 域服务对象	12
1.2.5 AD DS 域服务组成结构	14
1.3 部署全新 AD DS 域服务	16
1.4 部署额外域控制器	21
1.4.1 网络参数设置	21
1.4.2 登录成员服务器	21
1.5 小 结	24
1.6 习 题	24
1.7 实 验	25
第 2 章 升级域控制器	26
2.1 功能级别	27
2.1.1 域功能级别	27
2.1.2 林功能级别	27
2.1.3 Windows Server 2008 域功能级别	28
2.1.4 域和林功能级别提升原则	29
2.2 操作主机角色	30
2.2.1 角色分类	30
2.2.2 角色功能简介	31
2.2.3 角色转移	32
2.2.4 部署架构	33
2.3 提升 Windows Server 2003 功能级别	34
2.3.1 提升 Windows Server 2003 域功能级别	34
2.3.2 提升 Windows Server 2003 林功能级别	35
2.3.3 拓展 Windows Server 2003 域架构	36

2.4	提升 Windows Server 2008 服务器为主域控制器	37
2.4.1	独立服务器参数设置	37
2.4.2	独立服务器提升为额外域控制器	37
2.4.3	占用操作主机角色	37
2.5	Windows Server 2003 域控制器降级	40
2.5.1	域控制器降级为成员服务器	40
2.5.2	成员服务器降级为独立服务器	42
2.6	小 结	42
2.7	习 题	42
2.8	实 验	43
第 3 章	域迁移	44
3.1	域迁移概述	45
3.1.1	迁移架构	45
3.1.2	迁移流程	45
3.1.3	DNS 解析	46
3.1.4	信任关系	46
3.2	域迁移准备	50
3.2.1	设置网络参数	50
3.2.2	提升功能级别	50
3.2.3	DNS 解析设置	51
3.2.4	创建域间信任关系	52
3.2.5	授予用户访问权限	54
3.3	部署 Active Directory 迁移	55
3.3.1	目标域部署 ADMT	55
3.3.2	安装“密码导出服务器服务”	56
3.4	域对象迁移	57
3.4.1	迁移用户	57
3.4.2	迁移计算机	59
3.4.3	迁移组	62
3.4.4	报告	64
3.5	小 结	66
3.6	习 题	66
3.7	实 验	66
第 4 章	管理计算机帐户	67
4.1	计算机帐户概述	68
4.1.1	计算机命名原则	68
4.1.2	计算机名类型	68
4.1.3	查看计算机名	69

4.1.4	计算机帐户密码	71
4.2	计算机帐户域处理权限	71
4.2.1	“将工作站添加到域”策略	71
4.2.2	“创建计算机对象”权限	73
4.3	计算机帐户升/降域	74
4.3.1	升域	74
4.3.2	降域	76
4.4	计算机帐户管理任务	77
4.4.1	创建计算机帐户	77
4.4.2	禁用计算机帐户	78
4.4.3	启用计算机帐户	78
4.4.4	删除计算机帐户	79
4.4.5	移动计算机帐户	79
4.4.6	添加计算机帐户到组	79
4.4.7	重设帐户	79
4.4.8	禁止更改计算机帐户密码	80
4.4.9	禁止删除计算机帐户	80
4.4.10	删除/禁用数周内没有登录的计算机帐户	81
4.4.11	域用户帐户与计算机帐户绑定	81
4.5	小 结	82
4.6	习 题	82
4.7	实 验	82
第 5 章	管理组 and 用户	83
5.1	组	84
5.1.1	组的类型	84
5.1.2	组作用域	84
5.1.3	组的部署原则	86
5.1.4	创建组	86
5.1.5	移动组	87
5.1.6	删除组	87
5.1.7	嵌套组	87
5.1.8	修改组	88
5.1.9	查看组的隶属关系	89
5.2	用 户	89
5.2.1	用户概述	90
5.2.2	用户命名和密码要求	90
5.2.3	用户权限和权利	91
5.2.4	创建域用户	94
5.2.5	创建企业管理员	95

5.2.6	添加用户到组	96
5.2.7	修改用户名称和密码	96
5.2.8	移动用户	97
5.2.9	删除和恢复用户	97
5.2.10	禁/启用帐户	98
5.2.11	用户主目录	99
5.3	用户配置文件	100
5.3.1	用户配置文件类型	100
5.3.2	用户配置文件存储位置	100
5.3.3	用户配置文件夹的其他文件	101
5.3.4	查看用户配置文件	102
5.3.5	漫游用户配置文件	102
5.4	小 结	105
5.5	习 题	106
5.6	实 验	106
第 6 章	管理组织单位	107
6.1	组织单位概述	108
6.1.1	组织单位模型	108
6.1.2	组织单位和组	108
6.2	组织单位规划	109
6.2.1	架构原则	109
6.2.2	架构模型	110
6.3	组织单位管理任务	113
6.3.1	创建组织单位	113
6.3.2	取消“防止容器被意外删除”安全选项	114
6.3.3	移动组织单位	114
6.3.4	重命名组织单位	115
6.3.5	删除组织单位	116
6.3.6	查找组织单位	116
6.3.7	取消权限继承	116
6.3.8	其他管理任务	117
6.4	小 结	117
6.5	习 题	118
6.6	实 验	118
第 7 章	部署子域与域树	119
7.1	基础知识	120
7.1.1	单域	120
7.1.2	子域	120

7.1.3	域树	121
7.1.4	域林	122
7.2	部署子域	123
7.2.1	部署子域	123
7.2.2	查看父子域信任关系	124
7.3	部署多域树	125
7.3.1	部署多域树	125
7.3.2	查看域树之间信任关系	127
7.4	部署信任关系	128
7.4.1	部署快捷信任	128
7.4.2	外部信任	130
7.4.3	森林信任	133
7.4.4	删除信任	134
7.5	小 结	134
7.6	习 题	135
7.7	实 验	135
第 8 章	部署只读域控制器	136
8.1	只读域控制器概述	137
8.1.1	RODC 的特性	137
8.1.2	密码复制策略	138
8.1.3	部署条件	140
8.1.4	准备用户和组	141
8.2	部署 RODC 域控制器	142
8.2.1	部署 RODC 域控制器	142
8.2.2	验证 RODC	146
8.3	RODC 域控制器管理任务	147
8.3.1	启用密码复制	148
8.3.2	查看缓存用户信息	148
8.3.3	预设密码	149
8.3.4	委派 RODC 域控制器管理权限	150
8.3.5	RODC 域控制器管理员验证	151
8.4	小 结	152
8.5	习 题	152
8.6	实 验	152
第 9 章	权限委派管理	154
9.1	委派概述	155
9.1.1	委派管理目标	155
9.1.2	委派阶段	156

9.1.3 委派原则	158
9.2 委派管理任务	158
9.2.1 委派组织单位	158
9.2.2 委派站点	160
9.2.3 委派组策略	161
9.2.4 受限委派	161
9.3 委派定制管理控制台	163
9.3.1 委派用户定制管理控制台	164
9.3.2 添加管理任务	166
9.4 小 结	167
9.5 习 题	168
9.6 实 验	168
第 10 章 组策略管理	169
10.1 组策略概述	170
10.1.1 组策略的功能	170
10.1.2 组策略分类	170
10.1.3 组策略的组件	170
10.1.4 组策略配置	172
10.1.5 组策略继承	173
10.2 部署组策略	173
10.2.1 创建组策略	173
10.2.2 编辑组策略	174
10.3 组策略管理任务	175
10.3.1 部署应用环境	175
10.3.2 脚本策略	175
10.3.3 发布安装软件	177
10.3.4 部署软件限制	179
10.3.5 文件夹重定向	180
10.3.6 受限制的组	182
10.3.7 文件系统	184
10.3.8 硬件访问控制策略	185
10.3.9 域密码策略	189
10.4 小 结	199
10.5 习 题	199
10.6 实 验	199
第 11 章 AGPM 高级组策略管理	201
11.1 基础知识	202
11.1.1 GPMC	202

11.1.2	AGPM 服务器组件	203
11.1.3	AGPM 客户端组件	203
11.1.4	联机模式	204
11.1.5	组策略对象类型	204
11.1.6	模板	205
11.1.7	组策略对象状态	206
11.1.8	记录跟踪	207
11.2	部署 AGPM 服务器组件	207
11.2.1	部署架构	207
11.2.2	部署前提条件	208
11.2.3	安装 AGPM 服务器	208
11.3	部署 AGPM 客户端组件	211
11.3.1	安装 AGPM 客户端计算机	211
11.3.2	配置电子邮件通知	213
11.3.3	委派访问权限	213
11.4	策略生命周期	214
11.4.1	创建模板	214
11.4.2	创建受控组策略对象	215
11.4.3	编辑受控组策略对象	217
11.4.4	部署受控组策略对象	219
11.4.5	发布受控组策略对象	220
11.4.6	删除受控组策略对象	220
11.5	小 结	221
11.6	习 题	222
11.7	实 验	222
第 12 章	部署首选项	223
12.1	基础知识	224
12.1.1	首选项支持的操作系统	224
12.1.2	首选项特性	224
12.1.3	客户端计算机组件	225
12.1.4	首选项分类	225
12.1.5	首选项	226
12.1.6	首选项作用域	229
12.1.7	首选项处理方法	229
12.1.8	组策略管理控制台	230
12.1.9	“Windows 设置”首选项功能简介	230
12.1.10	“控制面板设置”首选项功能简介	232
12.2	部署“计算机配置”首选项	234
12.2.1	部署“Windows 设置”首选项	234

12.2.2	部署“控制面板设置”首选项	236
12.3	部署“用户设置”首选项	238
12.3.1	部署“Windows 设置”首选项	238
12.3.2	部署“控制面板设置”首选项	240
12.4	小 结	242
12.5	习 题	242
12.6	实 验	243
第 13 章	终端服务桌面应用	244
13.1	终端服务概述	245
13.1.1	终端服务简介	245
13.1.2	桌面虚拟化功能	246
13.2	安装终端服务	248
13.2.1	创建用户和组	248
13.2.2	安装“终端服务”角色	248
13.2.3	授权终端服务器	252
13.2.4	终端服务器配置	254
13.3	验证终端服务	257
13.4	在 Windows Server 2008 客户机上远程管理	258
13.5	使用 Web 方式远程管理	260
13.5.1	安装远程桌面 Web 连接组件	260
13.5.2	使用 IE 浏览器远程管理	262
13.6	应用程序虚拟化	264
13.6.1	发布应用程序	264
13.6.2	创建 RDP 文件	266
13.6.3	访问应用程序	267
13.7	使用终端服务网关	270
13.7.1	TS 网关概述	270
13.7.2	安装 TS 网关	271
13.7.3	为 TS 网关服务器获取证书	274
13.7.4	创建终端服务授权策略	275
13.7.5	配置终端服务客户端	279
13.8	小 结	282
13.9	习 题	282
13.10	实 验	282
第 14 章	用户隔离	284
14.1	基础知识	285
14.1.1	网络健康验证器	285
14.1.2	正常客户端计算机	285

14.1.3	非正常客户端计算机	285
14.1.4	更新服务器	285
14.1.5	网络策略	286
14.1.6	策略验证	286
14.1.7	隔离	286
14.1.8	补救	286
14.1.9	跟踪监控	287
14.1.10	客户端计算机代理	287
14.1.11	网络访问	287
14.1.12	部署环境	287
14.2	配置用户隔离服务器	294
14.2.1	配置 DHCP 服务器	295
14.2.2	配置网络限制策略	297
14.2.3	部署全局组策略	300
14.3	部署隔离策略	303
14.3.1	部署隔离没有加入域的笔记本电脑	303
14.3.2	部署防火墙隔离策略	307
14.3.3	部署“自动更新”隔离策略	311
14.3.4	部署补丁更新强制策略	313
14.4	小 结	315
14.5	习 题	315
14.6	实 验	316
第 15 章	管理 FSMO	317
15.1	FSMO 角色与部署	318
15.1.1	FSMO 角色概述	318
15.1.2	FSMO 部署	320
15.2	识别角色支持器	323
15.2.1	Active Directory 用户和计算机	323
15.2.2	Active Directory 域和信任	324
15.2.3	命令行选项	324
15.3	维护角色支持器	327
15.3.1	维护架构主机	327
15.3.2	维护域命名主机	329
15.3.3	维护基础结构主机	331
15.3.4	维护 RID 主机	333
15.3.5	维护 PDC 仿真主机角色	335
15.3.6	失败的角色支持器	336
15.4	小 结	337
15.5	习 题	337

15.6 实 验	338
第 16 章 活动目录数据库与备份	339
16.1 活动目录数据的管理	340
16.1.1 重定向 Active Directory 数据库	340
16.1.2 更改 Garbage Collection 代理的记录级别	341
16.1.3 离线整理 Active Directory 数据库	342
16.1.4 修复 Active Directory 数据库	343
16.1.5 Active Directory 数据库快照	344
16.1.6 重置目录服务还原模式管理员帐户密码	348
16.1.7 查找和清理重复的安全标识符	349
16.1.8 自动管理 Active Directory 数据库	350
16.2 活动目录数据库的备份与恢复	350
16.2.1 加载备份与恢复组件	351
16.2.2 备份活动目录数据库	352
16.2.3 恢复活动目录数据库	359
16.3 小 结	364
16.4 习 题	364
16.5 实 验	365
第 17 章 监控系统和活动目录	366
17.1 监控 Windows 系统性能	367
17.1.1 安装 Spotlight on Windows	367
17.1.2 启动 Spotlight on Windows	368
17.1.3 监控服务器性能	369
17.2 监控 Active Directory	376
17.2.1 安装“Spotlight On Active Directory”	376
17.2.2 监控 Active Directory	378
17.3 小 结	389
17.4 习 题	389
17.5 实 验	389
第 18 章 活动目录故障诊断与排除	390
18.1 Active Directory 故障诊断方法	391
18.1.1 故障发现和修复步骤	391
18.1.2 检查事件信息	395
18.1.3 寻找解决方案	396
18.1.4 尝试解决方案	397
18.1.5 检查“成功”	397
18.1.6 将发现写入文档	397

18.1.7	预防可能的故障	398
18.1.8	Active Directory 工具	398
18.2	排除基础服务故障	399
18.2.1	基本的故障排除工具	400
18.2.2	DNS 故障排除工具	402
18.2.3	WINS 故障排除工具	406
18.3	排除活动目录故障	407
18.3.1	Active Directory 文件	407
18.3.2	排除 Active Directory 复制故障	410
18.3.3	排除 FSMO 角色的故障	415
18.3.4	排除登录失败故障	418
18.4	小 结	428
18.5	习 题	428
18.6	实 验	429
第 19 章	活动目录新技术	430
19.1	AD DS 域服务概述	431
19.1.1	AD DS 域服务的新增功能	431
19.1.2	活动目录的常用概念	434
19.2	AD DS 域服务的管理方式	437
19.2.1	AD DS 域服务的安装	437
19.2.2	站点的管理	438
19.3	Active Directory 轻型目录服务	444
19.3.1	AD LDS 概述	444
19.3.2	安装 AD LDS	445
19.3.3	创建 AD LDS 实例	446
19.3.4	管理 AD LDS	449
19.4	组策略管理	454
19.4.1	组策略管理控制台	454
19.4.2	组策略继承	455
19.4.3	组策略委派	456

第1章

部署 AD DS 域服务

Windows Server 2003 中被人们所熟知的活动目录 (Active Directory)，在 Windows Server 2008 中被称为活动目录域服务 (Active Directory Domain Services, AD DS)，意指存储网络资源信息的目录。归根结底，活动目录就是一种数据库，网络中所有的资源，包括用户账户、文件数据、服务器、数据库、计算机、组织单位以及安全策略等信息都可以存在于活动目录中，从而使用户的使用和管理变得更加简单和方便。

本章导读

- 安装 Windows Server 2008
- AD DS 服务器角色
- AD DS 域服务对象和组成结构
- 部署全新 AD DS 域服务
- 部署额外域控制器