

目 录

第 1 章 Active Directory 域服务 (AD DS)	1
1.1 Active Directory 域服务概述	2
1.1.1 Active Directory 域服务的适用范围 (Scope)	2
1.1.2 名称空间 (Namespace)	2
1.1.3 对象 (Object) 与属性 (Attribute)	3
1.1.4 容器 (Container) 与组织单位 (Organization Units, OU)	3
1.1.5 域树 (Domain Tree)	4
1.1.6 信任 (Trust)	5
1.1.7 林 (Forest)	5
1.1.8 架构 (Schema)	6
1.1.9 域控制器 (Domain Controller)	6
1.1.10 只读域控制器 (RODC)	7
1.1.11 可重启的 AD DS (Restartable AD DS)	9
1.1.12 Active Directory 回收站	9
1.1.13 AD DS 的复制模式	9
1.1.14 域中的其他成员计算机	10
1.1.15 DNS 服务器	11
1.1.16 轻型目录访问协议 (LDAP)	11
1.1.17 全局编录 (Global Catalog)	12
1.1.18 站点 (Site)	12
1.1.19 目录分区 (Directory Partition)	13
1.2 域功能级别与林功能级别	14
1.2.1 域功能级别 (Domain Functionality Level)	14
1.2.2 林功能级别 (Forest Functionality Level)	14
1.3 Active Directory 轻型目录服务	15
第 2 章 建立 AD DS 域	17
2.1 建立 AD DS 域前的准备工作	18
2.1.1 选择适当的 DNS 域名	18



2.1.2	准备好一台支持 AD DS 的 DNS 服务器	18
2.1.3	选择 AD DS 数据库的存储位置	20
2.2	建立 AD DS 域	21
2.3	确认 AD DS 域是否正常	27
2.3.1	检查 DNS 服务器内的记录是否完备	27
2.3.2	排除注册失败的问题	30
2.3.3	检查 AD DS 数据库文件与 SYSVOL 文件夹	30
2.3.4	新增的管理工具	32
2.3.5	查看事件日志文件	33
2.4	提升域与林功能级别	33
2.5	新建额外域控制器与 RODC	34
2.5.1	安装额外域控制器	35
2.5.2	利用安装媒体来安装额外域控制器	40
2.5.3	更改 RODC 的委派与密码复制策略设置	42
2.6	RODC 阶段式安装	44
2.6.1	建立 RODC 账户	44
2.6.2	将服务器附加到 RODC 账户	48
2.7	将 Windows 计算机加入或脱离域	51
2.7.1	将 Windows 计算机加入域	52
2.7.2	利用已加入域的计算机登录	55
2.7.3	脱机加入域	57
2.7.4	脱离域	58
2.8	在域成员计算机内安装 AD DS 管理工具	59
2.9	删除域控制器与域	61
第 3 章	域用户与组账户的管理	66
3.1	管理域用户账户	67
3.1.1	创建组织单位与域用户账户	68
3.1.2	用户登录账户	69
3.1.3	创建 UPN 后缀	70
3.1.4	账户的常规管理工作	72
3.1.5	域用户账户的属性设置	73
3.1.6	搜索用户账户	75
3.1.7	域控制器之间数据的复制	80



3.2 一次同时新建多个用户账户	81
3.2.1 利用 csvde.exe 来新建用户账户	82
3.2.2 利用 ldifde.exe 来新建、修改与删除用户账户	83
3.2.3 利用 dsadd.exe 等程序添加、修改与删除用户账户	84
3.3 域组账户	86
3.3.1 域内的组类型	86
3.3.2 组的作用域	86
3.3.3 域组的创建与管理	88
3.3.4 AD DS 内置的组	88
3.3.5 特殊组账户	90
3.4 组的使用原则	91
3.4.1 A、G、DL、P 原则	91
3.4.2 A、G、G、DL、P 原则	91
3.4.3 A、G、U、DL、P 原则	92
3.4.4 A、G、G、U、DL、P 原则	92
第 4 章 利用组策略管理用户工作环境	93
4.1 组策略概述	94
4.1.1 组策略的功能	94
4.1.2 组策略对象	95
4.1.3 策略设置与首选项设置	98
4.1.4 组策略的应用时机	98
4.2 策略设置实例演练	99
4.2.1 策略设置实例演练一：计算机配置	99
4.2.2 策略设置实例演练二：用户配置	102
4.3 首选项设置实例演练	105
4.3.1 首选项设置实例演练一	105
4.3.2 首选项设置实例演练二	109
4.4 组策略的处理规则	112
4.4.1 一般的继承与处理规则	112
4.4.2 例外的继承设置	113
4.4.3 特殊的处理设置	116
4.4.4 更改管理 GPO 的域控制器	120
4.4.5 更改组策略的应用间隔时间	122

4.5	利用组策略来管理计算机与用户环境	124
4.5.1	计算机配置的管理模板策略	124
4.5.2	用户配置的管理模板策略	126
4.5.3	账户策略	127
4.5.4	用户权限分配策略	130
4.5.5	安全选项策略	132
4.5.6	登录/注销、启动/关机脚本	133
4.5.7	文件夹重定向	136
4.6	利用组策略限制访问可移动存储设备	142
4.7	WMI 筛选器	144
4.8	组策略建模与组策略结果	149
4.9	组策略的委派管理	154
4.9.1	站点、域或组织单位的 GPO 链接委派	155
4.9.2	编辑 GPO 的委派	155
4.9.3	新建 GPO 的委派	156
4.10	StarterGPO 的设置与使用	157
第 5 章	利用组策略部署软件	159
5.1	软件部署概述	160
5.1.1	将软件分配给用户	160
5.1.2	将软件分配给计算机	160
5.1.3	将软件发布给用户	160
5.1.4	自动修复软件	161
5.1.5	删除软件	161
5.2	将软件发布给用户	161
5.2.1	发布软件	161
5.2.2	客户端安装被发布的软件	164
5.2.3	测试自动修复软件的功能	165
5.2.4	取消已发布的软件	166
5.3	将软件分配给用户或计算机	167
5.3.1	分配给用户	167
5.3.2	分配给计算机	168
5.4	将软件升级	168
5.5	部署 Adobe Acrobat	172



5.5.1 部署基础版	172
5.5.2 部署更新程序	174
第 6 章 限制软件的运行	177
6.1 软件限制策略概述	178
6.1.1 哈希规则	178
6.1.2 证书规则	178
6.1.3 路径规则	179
6.1.4 网络区域规则	179
6.1.5 规则的优先级	179
6.2 启用软件限制策略	180
6.2.1 建立哈希规则	181
6.2.2 建立路径规则	183
6.2.3 建立证书规则	185
6.2.4 建立网络区域规则	188
6.2.5 不要将软件限制策略应用到本地系统管理员	188
第 7 章 建立域树与林	190
7.1 建立第一个域	191
7.2 建立子域	191
7.3 建立林中的第二个域树	198
7.3.1 选择适当的 DNS 架构	198
7.3.2 建立第二个域树	200
7.4 删除子域与域树	206
7.5 更改域控制器的计算机名称	210
第 8 章 管理域与林信任	214
8.1 域与林信任概述	215
8.1.1 信任域与受信任域	215
8.1.2 跨域访问资源的流程	215
8.1.3 信任的种类	218
8.1.4 建立信任前的注意事项	221
8.2 建立快捷方式信任	223
8.3 建立林信任	229



8.3.1	建立林信任前的注意事项	229
8.3.2	开始建立林信任	230
8.3.3	选择性身份验证设置	238
8.4	建立外部信任	240
8.5	管理与删除信任	242
8.5.1	信任的管理	242
8.5.2	信任的删除	244
第 9 章	AD DS 数据库的复制	247
9.1	站点与 AD DS 数据库的复制	248
9.1.1	同一个站点之间的复制	248
9.1.2	不同站点之间的复制	250
9.1.3	目录分区与复制拓扑	251
9.1.4	复制通信协议	251
9.2	默认站点的管理	252
9.2.1	默认的站点	252
9.2.2	Servers 文件夹与复制设置	253
9.3	利用站点来管理 AD DS 复制	256
9.3.1	建立站点与子网	257
9.3.2	建立站点链接	259
9.3.3	将域控制器移动到所属的站点	261
9.3.4	指定首选的 bridgehead 服务器	262
9.3.5	站点链接与 AD DS 数据库的复制设置	264
9.3.6	站点链接桥	265
9.3.7	站点链接桥的两个范例讨论	267
9.4	管理全局编录服务器	269
9.4.1	向全局编录内添加属性	270
9.4.2	全局编录的功能	270
9.4.3	通用组成员缓存	272
9.5	解决 AD DS 复制冲突的问题	274
9.5.1	属性标记	274
9.5.2	冲突的种类	274



第 10 章 操作主机的管理	278
10.1 操作主机概述	279
10.1.1 架构操作主机	279
10.1.2 域命名操作主机	279
10.1.3 RID 操作主机	280
10.1.4 PDC 模拟器操作主机	280
10.1.5 基础结构操作主机	283
10.2 操作主机的放置优化	284
10.2.1 基础结构操作主机的放置	284
10.2.2 PDC 模拟器操作主机的放置	284
10.2.3 林级别操作主机的放置	285
10.2.4 域级别操作主机的放置	285
10.3 找出扮演操作主机角色的域控制器	286
10.3.1 利用管理控制台找出扮演操作主机的域控制器	286
10.3.2 利用命令找出扮演操作主机的域控制器	288
10.4 转移操作主机角色	289
10.4.1 利用管理控制台	290
10.4.2 利用 Windows PowerShell 命令	292
10.5 夺取操作主机角色	293
10.5.1 操作主机停摆所造成的影响	293
10.5.2 夺取操作主机角色实例演练	295
第 11 章 AD DS 的维护	297
11.1 系统状态概述	298
11.1.1 AD DS 数据库	298
11.1.2 SYSVOL 文件夹	299
11.2 备份 AD DS	299
11.2.1 安装 Windows Server Backup 功能	299
11.2.2 备份系统状态	300
11.3 还原 AD DS	303
11.3.1 进入目录服务修复模式的方法	303
11.3.2 执行 AD DS 的非授权还原	304
11.3.3 针对被删除的 AD DS 对象执行授权还原	309



11.4	AD DS 数据库的移动与整理	312
11.4.1	可重新启动的 AD DS (Restartable AD DS)	313
11.4.2	移动 AD DS 数据库文件	313
11.4.3	重整 AD DS 数据库	317
11.5	重置“目录服务修复模式”的系统管理员密码	320
11.6	更改可重新启动的 AD DS 的登录设置.....	321
11.7	Active Directory 回收站	322
第 12 章	将资源发布到 AD DS.....	326
12.1	将共享文件夹发布到 AD DS	327
12.1.1	利用 Active Directory 用户和计算机控制台	327
12.1.2	利用计算机管理控制台	329
12.2	查找 AD DS 内的资源	329
12.2.1	通过网络	330
12.2.2	通过 Active Directory 用户和计算机控制台	331
12.3	将共享打印机发布到 AD DS	332
12.3.1	发布打印机.....	332
12.3.2	通过 AD DS 查找共享打印机	333
12.3.3	利用打印机位置来查找打印机	333
第 13 章	自动信任根 CA	338
13.1	自动信任 CA 的设置准则.....	339
13.2	自动信任内部的独立 CA.....	339
13.2.1	下载独立根 CA 的证书并保存.....	340
13.2.2	将 CA 证书导入到受信任的根证书颁发机构	341
13.3	自动信任外部的 CA.....	344
13.3.1	下载独立根 CA 的证书并保存.....	344
13.3.2	建立证书信任列表 (CTL)	347
附录 A	AD DS 与防火墙	351
A.1	AD DS 相关的端口.....	352
A.1.1	将客户端计算机加入域、用户登录时会用到的端口	352
A.1.2	计算机登录时会用到的端口	353
A.1.3	建立域信任时会用到的端口	353



A.1.4	验证域信任时会用到的端口	353
A.1.5	访问文件资源时会用到的端口	354
A.1.6	执行 DNS 查询时会用到的端口	354
A.1.7	执行 AD DS 数据库复制时会用到的端口	354
A.1.8	文件复制服务 (FRS) 会用到的端口	354
A.1.9	分布式文件系统 (DFS) 会用到的端口	355
A.1.10	其他可能需要开放的端口	355
A.2	限制动态 RPC 端口的使用范围	356
A.2.1	限制所有服务的动态 RPC 端口范围	356
A.2.2	限制 AD DS 数据库复制使用指定的静态端口	357
A.2.3	限制 FRS 使用指定的静态端口	358
A.2.4	限制 DFS 使用指定的静态端口	359
A.3	IPSec 与 VPN 端口	360
A.3.1	IPSec 所使用的通信协议与端口	360
A.3.2	PPTP VPN 所使用的通信协议与端口	361
A.3.3	L2TP/IPSec 所使用的通信协议与端口	361
附录 B	Server Core 与 Nano 服务器	362
B.1	Server Core 服务器概述	363
B.2	Server Core 服务器的基本设置	364
B.2.1	更改计算机名称	364
B.2.2	更改 IP 地址	365
B.2.3	启用 Server Core 服务器	367
B.2.4	加入域	367
B.2.5	将域用户加入本地 Administrators 组	368
B.2.6	更改日期与时间	369
B.3	在 Server Core 服务器内安装角色与功能	369
B.3.1	查看所有角色与功能的状态	369
B.3.2	DNS 服务器角色	370
B.3.3	DHCP 服务器角色	371
B.3.4	文件服务角色	372
B.3.5	Hyper-V 角色	372
B.3.6	打印服务角色	373
B.3.7	Active Directory 证书服务 (AD CS) 角色	373



B.3.8	Active Directory 域服务 (AD DS) 角色	373
B.3.9	Web 服务器 (IIS) 角色	373
B.4	远程管理 Server Core 服务器	374
B.4.1	通过服务器管理器来管理 Server Core 服务器	374
B.4.2	通过 MMC 管理控制台来管理 Server Core 服务器	378
B.4.3	通过远程桌面来管理 Server Core 服务器	379
B.4.4	硬件设备的安装	381
B.5	在虚拟机内运行的 Nano 服务器	382
B.5.1	建立供虚拟机使用的 Nano 服务器映像文件	382
B.5.2	建立与启动 Nano 服务器的虚拟机	385
B.5.3	将 Nano 服务器加入域	388
B.6	在物理机内运行的 Nano 服务器	392
B.6.1	建立供物理机使用的 Nano 服务器映像文件	393
B.6.2	利用 WinPE 启动计算机与安装 Nano 服务器	393