

北京科海培训中心

MCSE 认证实录

Microsoft Certified System Engineer

针对 MCSE 2000 考试的核心课程知识的详细介绍，包括：网络基础、网络管理、网络高级应用



北京科海集团公司 出品

北京科海培训中心

MCSE 认证实录

郭 庆 编著

北京科海集团公司 出品

2001.9

内 容 提 要

随着微软产品应用得越来越广泛,取得 MCSE (微软认证系统工程师) 的认证已经成为谋求一个好职位的有力凭证。本书不是根据具体的考试科目,而是根据核心考试的知识点来组织和编排的,使得读者能够更加有效地掌握核心考试所涉及的知识点。

全书共分 3 部分:第 1 部分“Windows 2000 Server&Professional”主要涵概了 70-210 和 70-215 考试中涉及的知识点;第 2 部分“基于 Windows 2000 的网络基础结构”主要涵概了 70-216 以及 70-221 考试中的知识点;第 3 部分“活动目录 (Active Directory) 的管理和规划”主要涵概了 70-217 和 70-219 考试中的知识点。而 70-240 和 70-220 考试所涉及的知识点在这 3 部分内容中都有所体现。

本书从易学的角度,尽可能地涵概 MCSE 认证核心考试所涉及的知识点,并且简单、准确地阐述其中涉及的重要概念,帮助读者快速、全面地掌握它们,以最快的速度切入到 MCSE 考试。通过学习这本书,读者可以具备构造基于 Windows 2000 的网络以及实施网络安全知识,可以深入了解 Windows 2000 的强大功能。因此本书除了可以用于 MCSE 认证考试的培训之外,也适用于希望深入掌握 Windows 2000 的读者。

品 名: MCSE 认证实录

作 者: 郭庆

责任编辑: 邱燕红

出 品: 北京科海集团公司

印 刷 者: 北京门头沟胶印厂

发 行: 新华书店总店北京科技发行所

开 本: 800×1000 1/16 印张: 26.375 字数: 571 千字

版 次: 2001 年 9 月第 1 版 2001 年 9 月第 1 次印刷

印 数: 1~5000

前 言

MCSE 是微软认证系统工程师的英文缩写，随着微软产品应用得越来越广泛，作为一名 IT 技术人员，取得 MCSE 的认证已经成为谋求一个好职位的有力凭证。原来以 Windows NT 4.0 为核心的 MCSE 考试已于 2000 年 12 月 31 日正式退役，取而代之的是 2000 年 8 月全面推出的 Windows 2000 Track MCSE 认证的考试。

Windows 2000 Track MCSE 认证要通过 7 门考试，它们分别是：4 门必考的 Windows 2000 核心考试、从 3 门 Windows 2000 核心考试中选考 1 门以及从任何有效的 MCSE 可选考试中选考 2 门。

其中 4 门必考的核心考试（对于通过了 Microsoft Windows NT 4.0 认证考试的人员，可以由一门升级考试 70-240 代替）为：

70-210: Installing, Configuring and Administering Microsoft Windows 2000 Professional

70-215: Installing, Configuring and Administering Microsoft Windows 2000 Server

70-216: Implementing and Administering a Microsoft Windows 2000 Network Infrastructure

70-217: Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure

70-240: Microsoft Windows 2000 Accelerated Exam for MCPs Certified on Microsoft Windows NT 4.0

可选的 Windows 2000 核心考试为下列 3 门考试中的任意 1 门：

70-219: Designing a Microsoft Windows 2000 Directory Services Infrastructure

70-220: Designing Security for a Microsoft Windows 2000 Network

70-221: Designing a Microsoft Windows 2000 Network Infrastructure

2 门任选考试为下列 10 门考试中任何有效的 2 门（不能与前面所选择的核心考试重复）：

70-028: System Administration for Microsoft SQL Server 7.0

70-029: Implementing a Database Design on Microsoft SQL Server 7.0

70-087: Microsoft Internet Information Server 4.0

70-081: Microsoft Exchange Server 5.5

70-079: Microsoft Internet Explorer 4.0

70-088: Implementing and Supporting Microsoft Proxy Server 2.0

70-219: Designing a Microsoft Windows 2000 Directory Services Infrastructure

70-220: Designing Security for a Microsoft Windows 2000 Network

70-221: Designing a Microsoft Windows 2000 Network Infrastructure

70-222: Upgrading from Microsoft Windows NT 4.0 to Microsoft Windows 2000

和其他的一些考试教材不同,本书不是根据具体的考试科目来组织和编排的,而是根据核心考试的知识点来组织和编排。因为各门考试科目之间的内容存在着交叉,如果按照考试科目来编排教材,必然会导致一些知识点的重复。同时,这些交叉的知识点又会成为学习过程中的难点。所以本书力求从知识点的角度来划分教材的编排结构,帮助读者更加有效地掌握核心考试所涉及的知识点。

从核心考试涉及的知识点来说,可以把 Windows 2000 分成 3 部分内容来介绍,它们分别是:

- (1) Windows 2000 Server & Professional;
- (2) 基于 Windows 2000 的网络基础结构;
- (3) 活动目录 (Active Directory) 的管理和规划。

其中第 1 部分“Windows 2000 Server&Professional”主要涵概了 70-210 和 70-215 考试中涉及的知识点,第 2 部分“基于 Windows 2000 的网络基础结构”主要涵概了 70-216 和 70-221 考试中的知识点,第 3 部分“活动目录 (Active Directory) 的管理和规划”主要涵概了 70-217 和 70-219 考试中的知识点。而 70-240 和 70-220 考试所涉及的知识点则在 3 部分内容中都有所体现,也就是说,这两门考试要求应试者对于 Windows 2000 系统有一个比较全面的认识和把握。

本书除了在编排上和其他教材不同之外,在内容上更加注重知识点的准确性和概念的简单性。在知其然和知其所以然的问题上,本书更加注重前者,目的是让读者能够快速掌握 MCSE 认证考试所涉及的知识点。至于很多知识点所涉及的原理,如果不妨碍读者掌握该知识点,本书都从略。

在笔者的教学实践中,发现很多学员更容易掌握和记住中文界面,因此本书中的图例都采用了中文界面。同时,采用中文界面的图例也十分有助于读者理解和掌握 Windows 2000 的各种功能,尤其有助于理解和掌握 Windows 2000 网络服务以及目录服务。因为实现一个服务可能会有很多细节,书中只能够有选择地介绍其中比较重要的内容,对于其他内容,读者则可以通过图例的中文界面直接了解到相应设置的功能,从而更加全面深入地了解 Windows 2000 的各种细节。此外,Windows 2000 的很多界面对于其中涉及的操作,甚至是其中涉及的一些基本概念,给予了一定的解释,把这些解释和课堂上教师介绍的英文界面对照,将非常有助于学员课下的复习和自学。

总之,本书针对要参加 Microsoft MCSE 认证考试的读者,从易学的角度,尽可能地涵概 MCSE 认证核心考试所涉及的知识点,并且简单、准确地阐述其中涉及的重要概念,帮助读者快速、全面地掌握它们,以最快的速度切入到 MCSE 考试。

同时,通过学习这本书,读者可以具备构造基于 Windows 2000 的网络以及实施网络安全知识,并且可以深入地了解 Windows 2000 强大功能。因此本书除了可以用于 MCSE 认证考试的培训之外,也适用于希望深入掌握 Windows 2000 的读者。

目 录

第 1 部分 Windows 2000 Server & Professional

第 1 章 网络基础	1
1.1 网络的基本类型	2
1.1.1 对等网 (Peer-to-Peer Network)	2
1.1.2 基于服务器的网络 (Server-Based Network)	3
1.1.3 网络的规模	4
1.1.4 网络拓扑	4
1.2 网络的连接	8
1.2.1 缆线的类型	8
1.2.2 网卡	13
1.2.3 数据的传输和访问	13
1.3 典型的局域网技术	15
1.3.1 以太网 (Ethernet) 标准	15
1.3.2 组建一个以太网	16
1.3.3 令牌环网 (Token Ring)	18
1.4 网络协议	19
1.4.1 常用的协议及特点	19
1.4.2 OSI 七层模型和 IEEE 802 模型简介	20
第 2 章 Windows 2000 的概述	23
2.1 Windows 2000 系列	23
2.1.1 工作站平台	23
2.1.2 服务器平台	24
2.2 全新安装 Windows 2000	25
2.2.1 最低配置	26
2.2.2 全新安装 Windows 2000	26
2.3 升级到 Windows 2000	32
2.3.1 升级路径	32

2.3.2 升级系统	33
2.4 配置双重启动	34
2.4.1 支持 Windows 2000 双重启动的操作系统	34
2.4.2 配置双重启动考虑的因素	34
2.4.3 配置双重启动	34
第 3 章 Windows 2000 的硬盘管理	37
3.1 Windows 2000 中硬盘的类型	37
3.1.1 基本硬盘	37
3.1.2 动态硬盘	39
3.2 在基本硬盘上建立分区	41
3.3 在动态硬盘上建立卷	42
3.3.1 将基本硬盘升级成为动态硬盘	42
3.3.2 将动态硬盘恢复成基本硬盘	42
3.3.3 建立和扩展简单卷	43
第 4 章 Windows 2000 的本地用户和组	44
4.1 用户帐号和组帐号概述	44
4.1.1 用户帐号概述	44
4.1.2 组帐号概述	45
4.1.3 用户配置文件 (User Profile)	45
4.1.4 本地用户和组的管理工具	47
4.2 本地用户帐号	50
4.2.1 内置的本地用户	50
4.2.2 创建本地用户帐号	50
4.2.3 用户帐号的删除和改名	51
4.2.4 设置本地用户属性	52
4.3 本地组帐号	55
4.3.1 内置的本地组	55
4.3.2 本地组的管理	56
第 5 章 Windows 2000 的文件管理	59
5.1 Windows 2000 文件系统概述	59
5.1.1 FAT 文件系统	59
5.1.2 FAT32 文件系统	59
5.1.3 NTFS 文件系统	60
5.1.4 FAT 或者 FAT32 向 NTFS 的转换	60
5.2 NTFS 文件系统	60

5.2.1 访问控制列表 (ACL, Access Control List)	61
5.2.2 NTFS 文件夹权限和文件权限	61
5.2.3 多重 NTFS 权限和权限的继承	62
5.2.4 实施 NTFS 权限	64
5.3 磁盘配额	69
5.3.1 Windows 2000 磁盘配额的特点	69
5.3.2 设置磁盘配额	70
5.4 文件共享	72
5.4.1 共享的管理	73
5.4.2 共享权限	77
第 6 章 打印机的安装与共享	80
6.1 Windows 2000 中打印机概述	80
6.1.1 打印的基本概念	80
6.1.2 打印的新特性及优点	81
6.1.3 打印过程	82
6.2 安装打印机	83
6.2.1 规划打印服务器的安装策略	83
6.2.2 安装打印机	84
6.2.3 配置打印客户计算机	88
6.3 配置打印机	90
6.3.1 共享打印机	90
6.3.2 设置打印权限	90
6.3.3 设置打印优先级	92
6.4 配置打印池	93
6.5 更改后台打印文件夹	94
6.6 基于 Web 的打印	95
第 7 章 本地安全策略	97
7.1 本地安全策略的管理工具	97
7.2 帐户策略	98
7.2.1 密码策略	98
7.2.2 帐户锁定策略	99
7.3 本地策略	99
7.3.1 审核策略	100
7.3.2 用户权利	100
7.3.3 安全选项	103

7.4 策略模板	104
7.4.1 导入策略模板	104
7.4.2 导出策略模板	105

第 2 部分 利用 Windows 2000 实现网络基础结构

第 8 章 TCP/IP 协议	106
8.1 TCP/IP 的概念及历史	106
8.1.1 数据传输过程	107
8.1.2 TCP/IP 协议组结构	107
8.2 TCP/IP 的应用层	109
8.3 TCP/IP 的传输层	111
8.3.1 TCP 协议	111
8.3.2 UDP 协议	114
8.4 TCP/IP 的 Internet 层	115
8.4.1 IP 协议	116
8.4.2 ICMP 协议	122
8.4.3 IGMP 协议	122
8.4.4 ARP 协议	123
8.5 TCP/IP 协议的网络接口层	125
8.5.1 NDIS 及网络连接方式	125
8.5.2 NDIS 驱动类型	127
8.6 配置本地连接的 TCP/IP 协议	127
8.6.1 动态配置方案	128
8.6.2 APIPA 方案	128
8.6.3 手动配置 IP 地址	129
8.6.4 使用 TCP/IP 命令工具	130
第 9 章 DHCP 服务	133
9.1 DHCP 的工作过程	133
9.2 DHCP 服务安装、配置和授权	136
9.2.1 安装 DHCP 服务	136
9.2.2 DHCP 服务的授权	137
9.2.3 配置 DHCP 客户机	138
9.2.4 创建和配置作用域	139
9.3 路由 DHCP 网络的规划	148

9.4 DHCP 服务的维护	151
第 10 章 DNS 服务	154
10.1 DNS 概述	154
10.1.1 域名的命名方式	154
10.1.2 域名的解析	154
10.2 DNS 服务的配置及安装	157
10.2.1 DNS 服务的安装	157
10.2.2 区域的概念	157
10.2.3 资源记录的概念	159
10.2.4 创建区域	161
10.2.5 配置区域传送	164
10.2.6 区域委派	170
10.2.7 配置动态更新区域	170
10.2.8 Internet 上的 DNS 配置	173
10.3 Active Directory 中的 DNS	174
10.4 DNS 的测试和排错	176
10.4.1 测试 DNS 服务查询	176
10.4.2 监视 DNS 服务	177
10.4.3 使用命令行检测 DNS 服务	177
第 11 章 WINS 服务	180
11.1 NetBIOS 名概述	180
11.2 WINS 概述	183
11.3 WINS 的安装和配置	186
11.3.1 WINS 服务器的安装	186
11.3.2 配置静态映射	186
11.3.3 WINS 代理	188
11.3.4 WINS 服务器配置	189
11.3.5 对 WINS 客户的配置	191
11.4 WINS 与 DNS 的集成	193
11.5 WINS 数据库的复制	196
11.5.1 WINS 数据库复制概述	196
11.5.2 配置 WINS 数据库复制	197
11.6 WINS 数据库的维护	200
11.6.1 WINS 数据库的一致性检查	200
11.6.2 WINS 数据库压缩	201

11.6.3	WINS 数据库的备份和恢复	201
第 12 章	Windows 2000 中的远程访问服务	203
12.1	远程访问服务简介	203
12.1.1	远程访问简介	203
12.1.2	拨号远程访问的组件	204
12.1.3	PPP 协议	209
12.1.4	远程访问服务器的结构	210
12.2	设置远程访问服务	211
12.2.1	配置远程访问客户机	211
12.2.2	设置远程访问服务器	216
12.2.3	Multilink 设置	220
12.2.4	验证协议(Authentication Protocols)	221
12.2.5	远程访问和 TCP/IP	224
12.3	管理远程访问	226
12.3.1	远程访问策略简介	226
12.3.2	远程访问策略原理	226
12.3.3	设置远程策略	229
12.3.4	远程访问的排错与优化	233
12.4	虚拟专用网	236
12.4.1	VPN 概述	236
12.4.2	管道协议 (Tunneling Protocol)	240
12.4.3	配置 VPN 服务器	240
12.4.4	设置远程访问客户机	242
12.4.5	加密协议 (Encryption Protocols)	243
12.4.6	路由和地址分配	244
第 13 章	Windows 2000 中的路由	247
13.1	路由器和路由表	247
13.1.1	路由术语	247
13.1.2	路由器的特点	248
13.1.3	Windows 2000 路由器	248
13.2	设置静态路由	250
13.2.1	查看静态路由表	250
13.2.2	添加静态路由	251
13.3	设置路由协议	252
13.3.1	路由协议	252

13.3.2	RIP 操作	252
13.3.3	添加 RIP 协议	254
13.3.4	添加支持 RIP 的接口	255
13.3.5	设置 RIP 接口	255
13.4	请求拨号路由	256
13.4.1	请求拨号路由概述	256
13.4.2	请求拨号路由组件	258
13.4.3	设置请求拨号路由	259
13.5	网络地址翻译 (NAT)	267
13.5.1	NAT 简介	268
13.5.2	NAT 工作原理	269
13.5.3	设置 NAT 服务器	270
13.5.4	设置 NAT 客户机	276
第 14 章	Internet 验证服务(IAS).....	277
14.1	IAS 服务简介	277
14.1.1	IAS 服务的优点	278
14.1.2	IAS 的应用	279
14.2	IAS 服务的验证过程	279
14.3	安装和设置 IAS 服务	280
14.3.1	安装 IAS 服务器	280
14.3.2	授权 IAS 服务	281
14.3.3	设置 IAS 客户	282
14.3.4	设置计帐信息的日志	283
14.3.5	设置 RADIUS 客户端	285
第 15 章	Windows 2000 的证书服务	288
15.1	公钥基础结构 (PKI) 概述	288
15.1.1	公钥加密技术	288
15.1.2	证书和证书颁发机构	289
15.1.3	Windows 2000 公钥基础结构组件	289
15.1.4	证书的层次模型	290
15.2	部署证书颁发机构	291
15.2.1	证书颁发机构模型	291
15.2.2	证书颁发机构公钥的产生	293
15.2.3	设置证书颁发机构标识信息	293
15.2.4	数据存储位置	294

15.2.5	CA 证书的申請.....	294
15.2.6	备份证书颁发机构	295
15.3	证书的申請和查看	295
15.3.1	利用证书申請向导申請证书	295
15.3.2	通过 Web 服务來申請证书	298
15.3.3	查看证书	299
15.4	证书的管理	301
15.4.1	颁发证书	301
15.4.2	吊銷证书	301
15.4.3	发布证书吊銷列表	302
15.4.4	导入和导出证书	304
第 16 章	网际协议安全 (IPSec)	309
16.1	IPSec 概述	309
16.1.1	常见的网络攻击	309
16.1.2	网络中 IPSec 的角色	310
16.1.3	安全关联 (SA)	310
16.1.4	IPSec 策略	311
16.2	实现 IPSec	311
16.2.1	添加 “IP 安全策略管理” 单元	312
16.2.2	使用预定义 IPSec 策略	313
16.2.3	实施 IPSec 策略	314
16.2.4	IPSec 数据包的结构	314
16.2.5	定制 IPSec 策略	319
16.2.6	选择 IPSec 加密方法	322
16.3	IPSec 监视器	323
16.3.1	使用 IPSec 监视器	323
16.3.2	优化 IPSec 策略性能	324
16.4	网络协议安全性排错	324
16.4.1	问题分隔	325
16.4.2	检验策略	325
第 3 部分 活动目录管理和规划		
第 17 章	活动目录概述	327
17.1	活动目录的基本概念	327

17.1.1	活动目录中的对象	327
17.1.2	活动目录的架构	328
17.1.3	轻量目录访问协议 (LDAP)	328
17.2	活动目录的功能	329
17.2.1	组织功能	329
17.2.2	管理功能	330
17.2.3	控制功能	330
17.3	Windows 2000 域的概念	331
17.3.1	域在安全性上的意义	331
17.3.2	域在网络管理上的意义	331
17.4	树和森林的概念	331
17.4.1	树	331
17.4.2	森林	332
第 18 章	建立域控制器	334
18.1	域控制器	334
18.1.1	活动目录复制	334
18.1.2	单主机操作	335
18.1.3	域控制器与普通服务器的区别	335
18.1.4	特殊的域控制器角色	335
18.2	建立域控制器的准备条件	337
18.3	为创建域配置 DNS	337
18.3.1	安装和配置 DNS	338
18.3.2	验证 DNS 服务器已经被授权	339
18.3.3	在活动目录安装的过程中安装 DNS	340
18.4	提升域控制器	340
18.5	将域控制器降级为普通服务器	342
18.6	添加副本域控制器	342
18.7	检查安装结果	343
18.7.1	验证 SRV 记录	343
18.7.2	验证 SYSVOL	344
18.7.3	验证目录数据库和日志文件	345
第 19 章	管理活动目录中的对象	347
19.1	域用户和组	347
19.1.1	组的类型和作用域	347
19.1.2	用户和组的关系	348

19.2	组织单元	349
19.2.1	用组织单元组织域中的对象	350
19.2.2	委派控制	351
19.3	Windows 2000 的访问控制部件	353
19.3.1	安全标识符 (SID, Security Identifier)	354
19.3.2	访问令牌 (Access token)	355
19.3.3	身份模仿级别及配置	356
19.3.4	安全描述符 (Security Descriptor)	358
19.3.5	访问控制列表 (ACL, Access Control List)	360
19.4	组策略概述	362
19.4.1	组策略对象	363
19.4.2	组策略对象链接	363
19.5	组策略的建立	363
19.5.1	新建组策略	363
19.5.2	删除组策略对象链接	364
19.5.3	添加组策略对象链接	364
19.6	组策略的配置	366
19.6.1	管理模板	367
19.6.2	安全设置	367
19.6.3	软件安装设置	369
19.6.4	脚本	369
19.6.5	文件夹的重定向	369
19.7	组策略的生效	371
19.7.1	组策略生效的范围	372
19.7.2	组策略对象的许可	372
19.7.3	用户的策略设置来源	373
19.7.4	策略的生效顺序	373
19.7.5	阻止继承和禁止替代组策略	374
第 20 章	活动目录的复制	376
20.1	活动目录复制的目的	376
20.2	活动目录复制的发生	377
20.3	活动目录复制的要素	377
20.3.1	复制的路径	377
20.3.2	复制的时间	378
20.3.3	复制的效率	378
20.3.4	冲突的解决	379

20.4 目录复制的内容	381
20.5 配置连接对象	381
第 21 章 管理活动目录站点	384
21.1 活动目录站点概述	384
21.1.1 站点的定义	384
21.1.2 站点的作用	386
21.2 建立站点	387
21.3 站点中的对象	388
21.4 站点和活动目录复制	389
21.4.1 站点链接	389
21.4.2 桥头服务器 (Bridgehead Server)	391
21.4.3 IP 和 SMTP 方式	392
21.4.4 站点链接桥 (Site Link Bridge)	392
21.5 站点和子网	394
21.6 在站点中放置服务器	395
第 22 章 操作主机 (Operations Master)	397
22.1 操作主机的概念	397
22.2 架构主机 (Schema master)	398
22.2.1 配置 “Active Directory 架构” 管理工具	398
22.2.2 查看和转移操作主机身份	398
22.3 域名主机 (Domain Naming Master)	400
22.3.1 查看域名主机身份	400
22.3.2 转移域名主机身份	400
22.4 PDC 模拟主机 (Primary Domain Controller Emulator Master)	401
22.5 RID 主机 (Relative Identifier Master)	403
22.6 基础主机 (Infrastructure Master)	403
22.7 操作主机的故障恢复	404

第 1 部分 Windows 2000 Server & Professional

第 1 章 网络基础

Windows 2000 是网络操作系统，它的很多功能都和网络相关。因此，在深入学习 Windows 2000 之前，本章先介绍一些网络的基础知识。

一些相互连接的计算机的集合，如图 1.1 所示，就构成了计算机网络。这些计算机之间的连接不一定要有电缆等线路连接，有的时候它们之间还可以由无线技术连接，这样连接着的计算机也可以构成计算机网络。所以只要是彼此互相连接的计算机就可以称为计算机网络。把计算机连接成一个网络之后可以达到资源共享，使通讯变得更简单等目的。

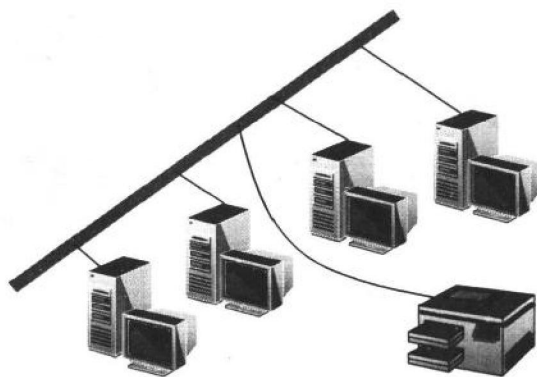


图 1.1 计算机网络示意图

如果没有网络，那么，要在任何一台计算机上进行打印时，打印机都必须连接到本地的计算机上才可以。除了打印机之外，通过网络还可以共享绘图仪、传真机、调制解调器等硬件设备。共享这些硬件设备可以避免对那些非必须硬件设备的重复投入。

另外，网络还为数据共享、软件共享提供了方便。而且通过网络我们可以很方便地把本计算机上的数据备份到网络上的其他计算机，为计算机系统提供了更加可靠的保障。