

Inhaltsverzeichnis

Danksagung	xvii
Über dieses Buch	xix
Zielgruppe	xix
Voraussetzungen	xx
Über die Begleit-CD	xx
Aufbau dieses Buches	xxi
Teil 1: Selbststudium	xxi
Teil 2: Prüfungsvorbereitung	xxii
Hinweise	xxii
Typographische Konventionen	xxiii
Tastaturkonventionen	xxiv
Erste Schritte	xxiv
Hardwarevoraussetzungen	xxiv
Softwarevoraussetzungen	xxv
Installationsanweisungen	xxv
Das Microsoft Certified Professional-Programm	xxvi
Zertifizierungen	xxvii
Voraussetzungen für den Erhalt eines MCP-Zertifikats	xxvii
Technischer Support	xxviii
Support für die Evaluierungssoftware	xxix
Teil I Selbststudium	1
Kapitel 1 Planen und Konfigurieren einer Authentifizierungsstrategie	3
Bedeutung dieses Kapitels	4
Bevor Sie beginnen	5
Lektion 1: Verstehen der Komponenten eines Authentifizierungsmodells	6
Der Unterschied zwischen Authentifizierung und Autorisierung	6
Netzwerk-Authentifizierungssysteme	7
Speichern von Anmeldeinformationen	8
Authentifizierungsfunktionen von Windows Server 2003	9

Authentifizierungsprotokolle bei Windows Server 2003	10
LM-Authentifizierung	11
NTLM-Authentifizierung	12
Der Kerberos-Authentifizierungsvorgang	13
Speichern der lokalen Anmeldeinformationen	15
Programme zur Behandlung von Authentifizierungsproblemen	16
Lernzielkontrolle	17
Zusammenfassung der Lektion	17
Lektion 2: Planen und Implementieren einer Authentifizierungsstrategie	19
Gesichtspunkte bei der Einschätzung Ihrer Umgebung	19
Empfehlungen zur Erstellung einer starken Kennwortrichtlinie	20
Optionen für Kontosperrungsrichtlinien	23
Optionen für das Erstellen einer Kerberos-Richtlinie	24
Windows 2003-Authentifizierungsmethoden für ältere Betriebssysteme	25
Verwenden der Multifaktor-Authentifizierung	29
Praktische Übung: Einstellen der Authentifizierungsoptionen	30
Lernzielkontrolle	32
Zusammenfassung der Lektion	33
Lektion 3: Konfigurieren der Authentifizierung für Webbenutzer	35
Konfigurieren des anonymen Zugriffs für Webbenutzer	35
Konfigurieren der Webauthentifizierung	36
Delegierte Authentifizierung	37
Praktische Übung: Konfigurieren der anonymen Authentifizierung	39
Lernzielkontrolle	43
Zusammenfassung der Lektion	44
Lektion 4: Erstellen von Vertrauensstellungen unter Windows Server 2003	45
Vertrauensstellungen in Windows Server 2003	47
Praktische Übung: Einrichten von Vertrauensstellungen	54
Lernzielkontrolle	59
Zusammenfassung der Lektion	61
Übung mit Fallbeispiel	62
Übung zur Problembehandlung	63
Zusammenfassung des Kapitels	65
Prüfungsrelevante Themen	67
Schlüsselthemen	67
Schlüsselbegriffe	67
Fragen und Antworten	68
Übung mit Fallbeispiel	72
Übung zur Problembehandlung	72

Kapitel 2 Planen und Konfigurieren einer Autorisierungsstrategie	75
Bedeutung dieses Kapitels	75
Bevor Sie beginnen	77
Lektion 1: Verstehen von Autorisierung	78
ACLs	78
Effektive Berechtigungen	80
Erben von Berechtigungen	80
Standardberechtigungen- und spezielle Berechtigungen	82
Praktische Übung: Verweigern des Zugriffs mithilfe von Gruppenmitgliedschaften	90
Lernzielkontrolle	93
Zusammenfassung der Lektion	94
Lektion 2: Verwalten von Gruppen unter Windows Server 2003	96
Gruppentypen unter Windows Server 2003	97
Gruppenbereiche	98
Domänen- und Gesamtstrukturfunktionsebenen	99
Vordefinierte Gruppen	101
Sondergruppen und -konten	105
Programme zur Administrierung von Sicherheitsgruppen	109
Erstellen der Richtlinie Eingeschränkte Gruppen	110
Praktische Übung: Erstellen von Gruppen und Zuweisen von Rechten	112
Lernzielkontrolle	113
Zusammenfassung der Lektion	114
Lektion 3: Planen, Implementieren und Verwalten einer Autorisierungsstrategie	116
Authentifizierung, Autorisierung und das Prinzip des geringsten Privilegs	116
Die Autorisierungsmethode Benutzer/ACL	117
Die Autorisierungsmethode Kontogruppe/ACL	118
Die Autorisierungsmethode Kontogruppe/Ressourcengruppe	118
Konventionen für Gruppennamen	119
Definieren, welche Benutzer Gruppen erstellen können	121
Verschachteln von Gruppen	122
Wann Gruppen zurückgezogen werden müssen	122
Lernzielkontrolle	123
Zusammenfassung der Lektion	124
Lektion 4: Behandlung von Autorisierungsproblemen	125
Behandlung einfacher Autorisierungsprobleme	125
Behandlung komplexer Autorisierungsprobleme	127
Lernzielkontrolle	133
Zusammenfassung der Lektion	133
Übung mit Fallbeispiel	134
Fallbeispiel	134
Fragen	134
Übung zur Problembehandlung	135
Fallbeispiel	135
Fragen	136

Zusammenfassung des Kapitels	137
Prüfungsrelevante Themen	139
Schlüsselthemen	139
Schlüsselbegriffe	139
Fragen und Antworten	140
Übung mit Fallbeispiel	143
Übung zur Problembehandlung	144
 Kapitel 3 Bereitstellung und Problembehandlung von Sicherheitsvorlagen	147
Bedeutung dieses Kapitels	148
Bevor Sie beginnen	148
Lektion 1: Konfigurieren von Sicherheitsvorlagen	150
Vordefinierte Sicherheitsvorlagen	151
Planen von Sicherheitsvorlagen	152
Erstellen und Bearbeiten von Sicherheitsvorlagen	153
Sicherheitsvorlageneinstellungen	156
Sicherheitskonfiguration für ältere Windows-Versionen	159
Praktische Übung: Erstellen und Prüfen einer neuen Sicherheitsvorlage	161
Lernzielkontrolle	163
Zusammenfassung der Lektion	164
Lektion 2: Bereitstellen von Sicherheitsvorlagen	165
Bereitstellen von Sicherheitsvorlagen mithilfe von Active Directory	165
Bereitstellen von Sicherheitsvorlagen ohne Active Directory	172
Praktische Übung: Anwenden und Bereitstellen von Sicherheitsvorlagen	174
Lernzielkontrolle	177
Zusammenfassung der Lektion	178
Lektion 3: Problembehandlung bei Sicherheitsvorlagen	179
Problembehandlung bei der Anwendung der Gruppenrichtlinien	179
Problembehandlung bei unerwarteten Sicherheitseinstellungen	187
Problembehandlung bei Systemrichtlinien	191
Lernzielkontrolle	193
Zusammenfassung der Lektion	194
Übung mit Fallbeispiel	194
Übung zur Problembehandlung	196
Zusammenfassung des Kapitels	198
Prüfungsrelevante Themen	199
Schlüsselthemen	199
Schlüsselbegriffe	199
Fragen und Antworten	200
Übung mit Fallbeispiel	202
Übung zur Problembehandlung	204

Kapitel 4 Absichern von Computern für bestimmte Rollen	205
Bedeutung dieses Kapitels	206
Bevor Sie beginnen	207
Lektion 1: Optimieren der Sicherheit für Clientrollen	208
Planen verwalteter Clientcomputer	209
Richtlinien für Software-Einschränkung	210
Sicherheitseinstellungen für Desktopcomputer	212
Sicherheit für mobile Computer	214
Sicherheit für Kiosks	214
Praktische Übung: Einschränken der Software	216
Lernzielkontrolle	219
Zusammenfassung der Lektion	220
Lektion 2: Optimieren der Sicherheit für Serverrollen	221
Firewalls	222
Perimeternetzwerke	226
Sicherheit für DHCP-Server	227
Sicherheit für DNS-Server	233
Sicherheit für Domänencontroller	236
Sicherheit für die Internetinformationsdienste	238
Sicherheit für den Internetauthentifizierungsdienst	247
Sicherheit für Exchange Server	250
Sicherheit für SQL Server	254
Praktische Übung: Absichern von Servern und Analysieren von Datenverkehr	258
Lernzielkontrolle	260
Zusammenfassung der Lektion	262
Lektion 3: Analysieren von Sicherheitskonfigurationen	263
Sicherheitskonfiguration und -analyse	263
Die grafikbasierte Oberfläche des Microsoft Baseline Security Analyzers	265
Die Befehlszeilenschnittstelle des Microsoft Baseline Security Analyzers	266
Praktische Übung: Analysieren von Sicherheitskonfigurationen	267
Lernzielkontrolle	269
Zusammenfassung der Lektion	269
Übung mit Fallbeispiel	270
Übung zur Problembehandlung	271
Zusammenfassung des Kapitels	273
Prüfungsrelevante Themen	275
Schlüsselthemen	275
Schlüsselbegriffe	275
Fragen und Antworten	277
Übung mit Fallbeispiel	279
Übung zur Problembehandlung	281

Kapitel 5 Planen einer Infrastruktur zur Updateverwaltung	283
Bedeutung dieses Kapitels	284
Bevor Sie beginnen	284
Lektion 1: Grundlagen zu Updates	285
Einführung in Updates	285
Updatetypen	286
Produktlebenszyklen	292
Verketteten von Updates	293
Lernzielkontrolle	294
Zusammenfassung der Lektion	295
Lektion 2: Update-Infrastruktur	296
Das Updateteam	296
Beurteilen der Umgebung	297
Bereitstellen von Updates	299
Die Updatetestumgebung	307
Praktische Übung: Auswerten der Update-Infrastruktur	308
Lernzielkontrolle	309
Zusammenfassung der Lektion	310
Lektion 3: Der Updatevorgang	311
Suchen von Updates	312
Auswerten von Updates	313
Abrufen von Updates	316
Testen von Updates	316
Installieren von Updates	317
Entfernen von Updates	317
Überwachen von Updates	319
Praktische Übung: Auswerten des Updatevorgangs	320
Lernzielkontrolle	320
Zusammenfassung der Lektion	321
Übung mit Fallbeispiel	322
Fallbeispiel	322
Fragen	324
Übung zur Problembehandlung	327
Zusammenfassung des Kapitels	328
Prüfungsrelevante Themen	329
Schlüsselthemen	329
Schlüsselbegriffe	329
Fragen und Antworten	331
Übung mit Fallbeispiel	334
Übung zur Problembehandlung	336

Kapitel 6 Bewerten und Bereitstellen einer Infrastruktur für die Patchverwaltung	339
Bedeutung dieses Kapitels	340
Bevor Sie beginnen	341
Lektion 1: Bewerten von Patchstufen	342
Die MBSA-Konsole	342
MBSACLI	345
Praktische Übung: Bewerten von Patchstufen im aktuellen Netzwerk	351
Lernzielkontrolle	353
Zusammenfassung der Lektion	354
Lektion 2: Bereitstellen von Updates auf neuen Clients	355
Überlegungen zur Sicherheit	355
Integrierte Installation	359
Skripting von Nicht-Microsoft-Updates	363
Praktische Übung: Erstellen einer integrierten Installation	364
Lernzielkontrolle	365
Zusammenfassung der Lektion	366
Lektion 3: Bereitstellen von Updates auf bestehenden Clients	367
Manuelles Ausführen von Updates	367
Windows Update-Website	369
Software Update Services	370
Client für automatische Updates	373
Gruppenrichtlinie	377
Praktische Übung: Konfigurieren von Software Update Services und des	
Clients für automatische Updates	379
Lernzielkontrolle	382
Zusammenfassung der Lektion	384
Übung mit Fallbeispiel	384
Fallbeispiel	384
Fragen	385
Übung zur Problembehandlung	386
Fallbeispiel	386
Fragen	388
Zusammenfassung des Kapitels	389
Prüfungsrelevante Themen	390
Schlüsselthemen	390
Schlüsselbegriffe	390
Fragen und Antworten	391
Übung mit Fallbeispiel	393
Übung zur Problembehandlung	394

Kapitel 7 Installieren, Konfigurieren und Verwalten von Zertifizierungsdiensten	397
Bedeutung dieses Kapitels	398
Bevor Sie beginnen	398
Lektion 1: Grundlagen zur öffentlichen Schlüsselinfrastruktur	399
Kryptografie und Verschlüsselung	399
Infrastruktur öffentlicher Schlüssel	401
Windows Server 2003-Zertifikatdienste	405
Praktische Übung: Konfigurieren einer Zertifizierungsstellenhierarchie	410
Lernzielkontrolle	414
Zusammenfassung der Lektion	415
Lektion 2: Verwalten von Zertifikatvorlagen	416
Übersicht über Zertifikatvorlagen	416
Zertifikatvorlagenversionen	418
Verwendung von Zertifikatvorlagen	418
Berechtigungen für Zertifikatvorlagen	422
Methoden für das Aktualisieren einer Zertifikatvorlage	423
Praktische Übung: Ablösen von Zertifikatvorlagen	425
Lernzielkontrolle	428
Zusammenfassung der Lektion	428
Lektion 3: Bereitstellen und Sperren von Zertifikaten	430
Zertifikatregistrierungsprozess	430
Methoden der Zertifikatregistrierung	431
Sperren von Zertifikaten	434
Veröffentlichen von Zertifikatsperrlisten	435
Problembehandlung beim Veröffentlichen von Zertifikatsperrlisten	438
Praktische Übung: Erstellen und Sperren von Zertifikaten	439
Lernzielkontrolle	444
Zusammenfassung der Lektion	445
Lektion 4: Archivieren und Wiederherstellen von Zertifikaten	446
Übersicht über die Schlüsselwiederherstellung	446
Exportieren von Schlüsseln	447
Schlüsselarchivierung	449
Schlüsselwiederherstellung	451
Praktische Übung: Exportieren und Wiederherstellen von Schlüsseln	453
Lernzielkontrolle	459
Zusammenfassung der Lektion	460
Übung mit Fallbeispiel	461
Fallbeispiel	461
Fragen	461
Übung zur Problembehandlung	462
Fallbeispiel	463
Übung 1: Reproduzieren des Problems	463
Fragen	464

Zusammenfassung des Kapitels	465
Prüfungsrelevante Themen	466
Fragen und Antworten	468
Übung mit Fallbeispiel	471
Übung zur Problembehandlung	472
 Kapitel 8 Planen und Konfigurieren von IPSec	 475
Bedeutung dieses Kapitels	476
Bevor Sie beginnen	477
Lektion 1: Grundlagen zu IPSec	478
IPSec-Überblick	478
Sichern von Host-zu-Host-Kommunikation	479
Sichern von Host-zu-Netzwerk-Kommunikation	481
Sichern von Netzwerk-zu-Netzwerk-Kommunikation	483
Aushandeln von IPSec-Verbindungen	485
Authentifizierungsheader und ESP	488
IPSec in Windows	488
Lernzielkontrolle	490
Zusammenfassung der Lektion	491
Lektion 2: Planen einer IPSec-Infrastruktur	492
Active Directory-Überlegungen	492
Authentifizierung für IPSec	493
Testen von IPSec	496
Lernzielkontrolle	497
Zusammenfassung der Lektion	498
Lektion 3: Konfigurieren von IPSec	499
IP-Filter	499
Filteraktionen	502
IP-Sicherheitsregeln	504
Konfigurieren von IP-Sicherheitsrichtlinien mit grafischen Programmen	505
Konfigurieren von IP-Sicherheitsrichtlinien mit Befehlszeilenprogrammen	507
Zertifikatssperrlisten-Überprüfung	508
Praktische Übung: Konfigurieren von IPSec-Richtlinien	509
Lernzielkontrolle	513
Zusammenfassung der Lektion	514
Übung mit Fallbeispiel	514
Fallbeispiel	515
Fragen	515
Übung zur Problembehandlung	516
Fallbeispiel	516
Fragen	516
Zusammenfassung des Kapitels	518

Prüfungsrelevante Themen	519
Schlüsselthemen	519
Schlüsselbegriffe	519
Fragen und Antworten	520
Übung mit Fallbeispiel	522
Übung zur Problembehandlung	523
 Kapitel 9 Bereitstellung und Problembehandlung bei IPSec	525
Bedeutung dieses Kapitels	526
Bevor Sie beginnen	526
Lektion 1: Bereitstellen von IPSec	528
Bereitstellung von IPSec unter Verwendung von Active Directory	528
Bereitstellen von IPSec mithilfe von Skripten	531
Bereitstellen von Zertifikatsdiensten für IPSec	535
Praktische Übung: Bereitstellen der IPSec-Konfigurationen	537
Lernzielkontrolle	541
Zusammenfassung der Lektion	542
Lektion 2: Überwachen von IPSec	543
IP-Sicherheitsmonitor-Snap-In	543
Ereignisanzeige	549
IKE-Ablaufverfolgung	554
Netsh	555
Konsole Leistung	555
Netzwerkmonitor	556
Netcap	558
Ping	558
IPSecMon	559
IPSecCmd	559
Netdiag	559
Praktische Übung: Überwachen von IPSec	560
Lernzielkontrolle	565
Zusammenfassung der Lektion	566
Lektion 3: Problembehandlung von IPSec	567
Allgemeine Problembehandlungs-Richtlinien	567
Kerberos-Authentifizierungsprobleme	568
Zertifikats-Authentifizierungsprobleme	569
Problembehandlung bei Firewalls, Routern und Paketfiltern	570
Netzwerkadressübersetzungs-Probleme	570
Kompatibilitätsprobleme	571
Lernzielkontrolle	573
Zusammenfassung der Lektion	573

Übung mit Fallbeispiel	574
Fallbeispiel	574
Fragen	574
Übung zur Problembehandlung	575
Fallbeispiel	575
Fragen	576
Zusammenfassung des Kapitels	577
Prüfungsrelevante Themen	578
Schlüsselthemen	578
Schlüsselbegriff	578
Fragen und Antworten	579
Entwurfsaktivität: Übung mit Fallbeispiel	581
Entwurfsaktivität: Übung zur Problembehandlung	582
 Kapitel 10 Planen und Implementieren der Sicherheit für drahtlose Netzwerke	 585
Bedeutung dieses Kapitels	586
Bevor Sie beginnen	586
Lektion 1: Grundlagen zur Sicherheit in drahtlosen Netzwerken	588
Sicherheitsrisiken	589
WEP	589
Wi-Fi Protected Access	597
Andere Techniken für Sicherheit in drahtlosen Netzwerken	599
Lernzielkontrolle	600
Zusammenfassung der Lektion	601
Lektion 2: Konfigurieren von drahtloser Sicherheit	602
Planen der Richtlinien für drahtlosen Zugriff	602
Entwerfen der Autorisierungsstrategie	604
Konfigurieren der Zertifikatsinfrastruktur	605
Konfigurieren von IAS	607
Konfigurieren eines Drahtlosnetzwerk-Clients	610
Konfigurieren von WAPs	615
Praktische Übung: Bereitstellen der WEP-Verschlüsselung mit PEAP-Authentifizierung	616
Lernzielkontrolle	621
Zusammenfassung der Lektion	622
Übung mit Fallbeispiel	622
Fallbeispiel	623
Fragen	623
Übung zur Problembehandlung	624
Fallbeispiel	624
Frage	625
Zusammenfassung des Kapitels	626

Prüfungsrelevante Themen	627
Schlüsselthemen	627
Schlüsselbegriffe	627
Fragen und Antworten	629
Entwurfsaktivität: Übung mit Fallbeispiel	630
Entwurfsaktivität: Übung zur Problembehandlung	631
 Kapitel 11 Bereitstellen, Konfigurieren und Verwalten von SSL-Zertifikaten	633
Bedeutung dieses Kapitels	634
Bevor Sie beginnen	634
Lektion 1: Übersicht über SSL (Secure Sockets Layer)	635
So funktioniert SSL	635
Vergleich von SSL mit IPSec	636
Beziehen von SSL-Zertifikaten	637
Erneuern von SSL-Zertifikaten	639
Konfigurieren von Firewalls	640
Lernzielkontrolle	640
Zusammenfassung der Lektion	642
Lektion 2: Konfigurieren von SSL für IIS	643
Verwenden von SSL-Zertifikaten für eine Website	643
Der Assistent für Webserverzertifikate	645
Clientzertifikate	650
Problembehandlung bei SSL	653
Praktische Übung: Verwenden von Zertifikaten für SSL	655
Lernzielkontrolle	659
Zusammenfassung der Lektion	660
Lektion 3: Andere SSL-Anwendungen	661
Aktivieren von SSL auf Active Directory-Domänencontrollern	661
Aktivieren von SSL auf Computern unter SQL Server	663
Aktivieren von SSL auf Mailservern	666
Aktivieren von SSL auf Microsoft Outlook	668
Praktische Übung: Schützen der Active Directory-Kommunikation	669
Lernzielkontrolle	673
Zusammenfassung der Lektion	674
Übung mit Fallbeispiel	674
Fallbeispiel	674
Fragen	675
Übung zur Problembehandlung	676
Fallbeispiel	677
Fragen	677
Zusammenfassung des Kapitels	678
Prüfungsrelevante Themen	679
Schlüsselthemen	679
Schlüsselbegriffe	679

Fragen und Antworten	680
Entwurfsaktivität: Übung mit Fallbeispiel	682
Entwurfsaktivität: Übung zur Problembehandlung	683
Kapitel 12 Sichern des Remotezugriffs	685
Bedeutung dieses Kapitels	686
Bevor Sie beginnen	687
Lektion 1: Grundlagen zum Remotezugriff	688
Remotezugriffsmethoden	688
VPN-Protokolle	690
Authentifizierungsmethoden	692
Lernzielkontrolle	699
Zusammenfassung der Lektion	700
Lektion 2: Konfigurieren von RAS-Servern	701
Konfigurieren der Authentifizierung	701
Konfigurieren der Autorisierung	703
Konfigurieren der Authentifizierung mit Zertifikaten oder Smartcards	707
Praktische Übung: Konfigurieren eines VPN-Servers und-Clients	708
Lernzielkontrolle	712
Zusammenfassung der Lektion	713
Lektion 3: Konfigurieren von RAS-Clients	714
Konfigurieren von clientseitigen Authentifizierungsprotokollen	714
VMVK-Assistent	716
Praktische Übung: Verwenden von VMVK	720
Lernzielkontrolle	725
Zusammenfassung der Lektion	726
Übung mit Fallbeispiel	726
Fallbeispiel	726
Fragen	726
Übung zur Problembehandlung	727
Fallbeispiel	727
Fragen	728
Zusammenfassung des Kapitels	729
Prüfungsrelevante Themen	730
Schlüsselthemen	730
Schlüsselbegriffe	730
Fragen und Antworten	732
Übung mit Fallbeispiel	734
Übung zur Problembehandlung	735

Teil II Prüfungsvorbereitung	737
Kapitel 13 Implementierung, Verwaltung und Problembehandlung bei Sicherheitsrichtlinien (1.0)	739
Geprüfte Fähigkeiten und vorgeschlagene praktische Übungen	740
Weiterführende Literatur	742
Kapitel 14 Implementierung, Verwaltung und Problembehandlung bei der Patchverwaltungsinfrastruktur (2.0)	783
Geprüfte Fähigkeiten und vorgeschlagene praktische Übungen	784
Weiterführende Literatur	785
Kapitel 15 Implementierung, Verwaltung und Problembehandlung bei der Sicherheit für die Netzwerkkommunikation (3.0)	819
Geprüfte Fähigkeiten und vorgeschlagene praktische Übungen	820
Weiterführende Literatur	824
Kapitel 16 Planung, Konfigurierung und Problembehandlung bei Authentifizierung, Autorisierung und PKI (4.0)	877
Geprüfte Fähigkeiten und vorgeschlagene praktische Übungen	879
Weiterführende Literatur	882
Glossar	917
Index	923
Systemvoraussetzungen	949