

MCTS (Exam 70-640)

Configuring Windows Server 2008 Active Directory

Self- Paced Training Kit

Holme, Dan	مؤلف: دان هولم، ۱۹۶۷-م
MCTS (Exam 70-640):	عنوان و نام پدیدآور:
Configuring Windows Server 2008 Active Directory Self- Paced Training Kit	
/Dan Holme, Nelson Ruest, Danielle Ruest	
مستندات نشر: تهران: مؤسسه فرهنگی هنری دیباگران تهران، ۱۳۹۰-۲۰۱۱م	
مستندات ظاهری: ۹۸۸ ص:، مصور.	
شابک: 978-0-7356-2513-6	
وضعیت فهرست نویسی: فبا	
یادداشت: انگلیسی	
آوانویسی عنوان: ام-سی-ان-اس-سلف- پیس-د ترینینگ کیت ...	
موضوع: ویندوز مایکروسافت سرور	
موضوع: نرم افزار مایکروسافت - آزمون ها - راهنمای مطالعه	
موضوع: داده پردازی - کارستان - گواهی نامه - راهنمای مطالعه	
شناسه افزوده: روست، نلسون	
شناسه افزوده: Ruest, Nelson	
شناسه افزوده: روست، دانیل	
شناسه افزوده: Ruest, Danielle	
شناسه افزوده: مؤسسه فرهنگی هنری دیباگران تهران	
رده بندی کنگره: ۹۱۳۹۰/۳۷۴۶/۳ QAY۶	
رده بندی دیویی: ۰۰۵/۴۴۷۶	
شماره کتبی شناسی ملی: ۲۳۸۸۴۲۸	

مؤلفان: Dan Holme- Nelson Ruest

Danielle Ruest

ناشر: مؤسسه فرهنگی هنری دیباگران تهران

چاپ: ادیبان ایران

نوبت چاپ: اول

تاریخ نشر: شهریور ماه ۱۳۹۰

تیراژ: ۵۰۰ نسخه

قیمت: ۲۴۰۰۰۰ ریال

شابک: ۹۷۸-۰-۷۳۵۶-۲۵۱۳-۶

ISBN: 978-0-7356-2513-6

نشانی دفتر مرکزی: تهران، سعادت آباد، میدان کاج، خ سرو شرقی، روبه روی خ علامه، پلاک ۴۹

وب سایت: dibagaran.mft.info

صندوق پستی: ۱۴۳۳۵/۹۴۳

نشانی واحد فروش: تهران، شهران، بالاتر از میدان دوم، نبش کوچه شهید عسگری، پلاک ۱۵۷

کد پستی: ۱۴۷۸۷۱۵۶۹۱

نمابر: ۴۴۳۰۸۸۸۸

تلفن: ۴۴۳۰۴۳۰۱-۵

فروش اینترنتی: www.mftshop.com

پست الکترونیکی: bookmarket@mftmail.com

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Copyright © 2008 by Dan Holme

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Control Number: 2008923653

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 QWE 3 2 1 0 9 8

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to tkinput@microsoft.com.

Microsoft, Microsoft Press, Access, Active Directory, ActiveX, BitLocker, Excel, Hyper-V, Internet Explorer, JScript, MSDN, Outlook, PowerPoint, SharePoint, SQL Server, Visio, Visual Basic, Windows, Windows Live, Windows NT, Windows PowerShell, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions Editor: Ken Jones

Developmental Editor: Laura Sackerman

Project Editor: Maureen Zimmerman

Editorial Production: nSight, Inc.

Technical Reviewers: Bob Hogan, Bob Dean; Technical Review services provided by Content Master, a member of CM Group, Ltd.

Cover: Tom Draper Design

Body Part No. X14-33191

About the Authors

Dan Holme

Dan Holme, a graduate of Yale University and Thunderbird, has spent more than a decade as a consultant and trainer, delivering solutions to tens of thousands of IT professionals from the most prestigious organizations and corporations around the world. Dan's company, Intelliem, specializes in boosting the productivity of IT professionals and end users by creating advanced, customized solutions that integrate clients' specific design and configuration into productivity-focused tools, training, and knowledge management services. Dan is also a contributing editor for *Windows IT Pro* magazine, an MVP (Office SharePoint Server), and the community lead of *officesharepointpro.com*. From his base in beautiful Maui, Dan travels around the globe supporting customers and delivering Windows technologies training. Immediately following the release of this Training Kit, he will be preparing for the Beijing Olympic Games as the Windows Technologies Consultant for NBC television, a role he also played in Torino in 2006.



Danielle Ruest

Danielle Ruest is passionate about helping people make the most of computer technology. She is a senior enterprise workflow architect and consultant with over 20 years of experience in project implementations. Her customers include governments and private enterprises of all sizes. Throughout her career, she has led change-management processes, developed and delivered training, provided technical writing services, and managed communications programs during complex technology implementation projects. More recently, Danielle has been involved in the design and support of test, development, and production infrastructures based on virtualization technologies. She is an MVP for the Virtual Machine product line.



Nelson Ruest

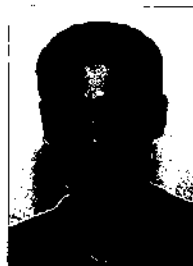
Nelson Ruest is passionate about doing things right with Microsoft technologies. He is a senior enterprise IT architect with over 25 years of experience. He was one of Canada's first Microsoft Certified Systems Engineers (MCSEs) and Microsoft Certified Trainers. In his IT career, he has been a computer operator, systems administrator, trainer, Help desk operator, support engineer, IT manager, project manager, and now, IT architect. He has also taken part in numerous migration projects, where he was responsible for everything from project management to systems design in both the private and public sectors. He is an MVP for the Windows Server product line.



Nelson and Danielle work for Resolutions Enterprises, a consulting firm focused on IT infrastructure design. Resolutions Enterprises can be found at <http://www.reso-net.com>. Both are authors of multiple books, notably the free *The Definitive Guide to Vista Migration* (<http://www.realtime-nexus.com/dgvm.htm>) and *Microsoft Windows Server 2008: The Complete Reference* (McGraw-Hill Osborne, 2008) (<http://www.mhprofessional.com/product.php?cat=112&isbn=0072263652>).

Tony Northrup

Tony Northrup, MVP, MCSE, MCTS, and CISSP, is a Windows consultant and author living in Phillipston, Massachusetts. Tony started programming before Windows 1.0 was released but has focused on Windows administration and development for the past 15 years. He has written more than a dozen books covering Windows networking, security, and development. Among other titles, Tony is coauthor of *Microsoft Windows Server 2003 Resource Kit* (Microsoft Press, 2005) and *Windows Vista Resource Kit* (Microsoft Press, 2007).



When he's not consulting or writing, Tony enjoys photography, remote-controlled flight, and golf. Tony lives with his cat, Sam, and his dog, Sandi. You can learn more about Tony by visiting his technical blog at <http://www.vistaclues.com> or his personal Web site at <http://www.northrup.org>.

Contents at a Glance

1	Installation	1
2	Administration	33
3	Users	85
4	Groups	139
5	Computers	187
6	Group Policy Infrastructure	229
7	Group Policy Settings	289
8	Authentication	355
9	Integrating Domain Name System with AD DS	393
10	Domain Controllers	459
11	Sites and Replication	507
12	Domains and Forests	555
13	Directory Business Continuity	607
14	Active Directory Lightweight Directory Services	685
15	Active Directory Certificate Services and Public Key Infrastructures	723
16	Active Directory Rights Management Services	781
17	Active Directory Federation Services	825
	Answers	875
	Index	921

Table of Contents

Introduction	xxix
Making the Most of the Training Kit	xxx
Setup and Hardware Requirements	xxx
Software Requirements and Setup	xxx
Using the CD	xxx
How to Install the Practice Tests	xxx
How to Use the Practice Tests	xxx
How to Uninstall the Practice Tests	xxx
Microsoft Certified Professional Program	xxx
Technical Support	xxx
1 Installation	1
Before You Begin	2
Lesson 1: Installing Active Directory Domain Services	3
Active Directory, Identity and Access	3
Beyond Identity and Access	8
Components of an Active Directory Infrastructure	8
Preparing to Create a New Windows Server 2008 Forest	11
Adding the AD DS Role Using the Windows Interface	12
Creating a Domain Controller	13
Creating a Windows Server 2008 Forest	14
Lesson Summary	21
Lesson Review	21

 **What do you think of this book? We want to hear from you!**

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

Lesson 2: Active Directory Domain Services on Server Core	23
Understanding Server Core	23
Installing Server Core	24
Performing Initial Configuration Tasks	25
Adding AD DS to a Server Core Installation	26
Removing Domain Controllers	26
Installing a Server Core Domain Controller	27
Lesson Summary	29
Lesson Review	30
Chapter Review	31
Key Terms	31
Case Scenario	32
Case Scenario: Creating an Active Directory Forest	32
Take a Practice Test	32
2 Administration	33
Before You Begin	33
Lesson 1: Working with Active Directory Snap-ins	35
Understanding the Microsoft Management Console	35
Active Directory Administration Tools	36
Finding the Active Directory Administrative Tools	37
Adding the Administrative Tools to Your Start Menu	37
Running Administrative Tools with Alternate Credentials	37
Creating a Custom Console with Active Directory Snap-ins	38
Saving and Distributing a Custom Console	39
Creating and Managing a Custom MMC	40
Lesson Summary	44
Lesson Review	45
Lesson 2: Creating Objects in Active Directory	46
Creating an Organizational Unit	46
Creating a User Object	48
Creating a Group Object	50
Creating a Computer Object	52
Finding Objects in Active Directory	54

Finding Objects by Using <i>Dsquery</i>	59
Understanding DNs, RDNs, and CNs.	60
Creating and Locating Objects in Active Directory.	61
Lesson Summary.	67
Lesson Review.	67
Lesson 3: Delegation and Security of Active Directory Objects.	69
Understanding Delegation.	69
Viewing the ACL of an Active Directory Object.	70
Object, Property, and Control Access Rights.	72
Assigning a Permission Using the Advanced Security Settings Dialog Box.	72
Understanding and Managing Permissions with Inheritance.	73
Delegating Administrative Tasks with the Delegation Of Control Wizard.	74
Reporting and Viewing Permissions.	75
Removing or Resetting Permissions on an Object.	75
Understanding Effective Permissions.	76
Designing an OU Structure to Support Delegation.	77
Delegating Administrative Tasks.	78
Lesson Summary.	79
Lesson Review.	80
Chapter Review.	81
Key Terms.	81
Case Scenario.	82
Case Scenario: Organizational Units and Delegation.	82
Suggested Practices.	82
Maintain Active Directory Accounts.	82
Take a Practice Test.	84
3 Users.	85
Before You Begin.	86
Lesson 1: Automating the Creation of User Accounts.	87
Creating Users with Templates.	87
Using Active Directory Command-Line Tools.	88
Creating Users with <i>Dsadd</i>	89
Importing Users with <i>CSVDE</i>	90

Importing Users with <i>LDIFDE</i>	90
Automating the Creation of User Accounts	93
Lesson Summary	96
Lesson Review	96
Lesson 2: Creating Users with Windows PowerShell and VBScript	98
Introducing Windows PowerShell	98
Understanding Windows PowerShell Syntax, Cmdlets, and Objects	99
Getting Help	101
Using Variables	102
Using Aliases	102
Namespaces, Providers, and PSDrives	103
Creating a User with Windows PowerShell	103
Importing Users from a Database with Windows PowerShell	106
Executing a Windows PowerShell Script	108
Introducing VBScript	108
Creating a User with VBScript	109
VBScript vs. Windows PowerShell	109
Creating Users with Windows PowerShell and VBScript	110
Lesson Summary	112
Lesson Review	112
Lesson 3: Supporting User Objects and Accounts	114
Managing User Attributes with Active Directory Users and Computers	114
Understanding Name and Account Attributes	118
Managing User Attributes with <i>Dismod</i> and <i>Dsget</i>	121
Managing User Attributes with Windows PowerShell and VBScript	123
Administering User Accounts	124
Supporting User Objects and Accounts	130
Lesson Summary	133
Lesson Review	133
Chapter Review	135
Key Terms	135
Case Scenario	136
Case Scenario: Import User Accounts	136

Suggested Practices	136
Automate the Creation of User Accounts	136
Maintain Active Directory Accounts	137
Take a Practice Test	137
4 Groups	139
Before You Begin	139
Lesson 1: Creating and Managing Groups	141
Managing an Enterprise with Groups	141
Defining Group Naming Conventions	143
Understanding Group Types	145
Understanding Group Scope	145
Converting Group Scope and Type	149
Managing Group Membership	151
Developing a Group Management Strategy	153
Creating and Managing Groups	155
Lesson Summary	156
Lesson Review	157
Lesson 2: Automating the Creation and Management of Groups	159
Creating Groups with <i>Dsadd</i>	159
Importing Groups with <i>CSVDE</i>	160
Managing Groups with <i>LDIFDE</i>	161
Retrieving Group Membership with <i>Dsget</i>	162
Changing Group Membership with <i>Dsmmod</i>	162
Moving and Renaming Groups with <i>Dsmove</i>	163
Deleting Groups with <i>Dsrm</i>	163
Managing Group Membership with Windows PowerShell and VBScript ...	164
Automating the Creation and Management of Groups	165
Lesson Summary	167
Lesson Review	167
Lesson 3: Administering Groups in an Enterprise	169
Best Practices for Group Attributes	169
Protecting Groups from Accidental Deletion	171
Delegating the Management of Group Membership	172

	Understanding Shadow Groups	176
	Default Groups	177
	Special Identities	179
	Administering Groups in an Enterprise	180
	Lesson Summary	181
	Lesson Review	182
	Chapter Review	184
	Key Terms	184
	Case Scenario	185
	Case Scenario: Implementing a Group Strategy	185
	Suggested Practices	185
	Automating Group Membership and Shadow Groups	186
	Take a Practice Test	186
5	Computers	187
	Before You Begin	188
	Lesson 1: Creating Computers and Joining the Domain	189
	Understanding Workgroups, Domains, and Trusts	189
	Identifying Requirements for Joining a Computer to the Domain	190
	Computers Container	190
	Creating OUs for Computers	190
	Delegating Permission to Create Computers	192
	Prestaging a Computer Account	192
	Joining a Computer to the Domain	193
	Importance of Prestaging Computer Objects	195
	Creating Computers and Joining the Domain	198
	Lesson Summary	201
	Lesson Review	202
	Lesson 2: Automating the Creation of Computer Objects	203
	Importing Computers with <i>CSVDE</i>	203
	Importing Computers with <i>LDIFDE</i>	204
	Creating Computers with <i>Dsadd</i>	205
	Creating Computers with <i>Netdom</i>	205
	Creating Computers with Windows PowerShell	206

Creating Computers with VBScript	208
Create and Manage a Custom MMC	209
Lesson Summary	211
Lesson Review	212
Lesson 3: Supporting Computer Objects and Accounts	213
Configuring Computer Properties	213
Moving a Computer	214
Managing a Computer from the Active Directory Users and Computers Snap-In	215
Understanding the Computer's Logon and Secure Channel	216
Recognizing Computer Account Problems	216
Resetting a Computer Account	217
Renaming a Computer	218
Disabling and Enabling Computer Accounts	219
Deleting Computer Accounts	220
Recycling Computers	220
Supporting Computer Objects and Accounts	221
Lesson Summary	222
Lesson Review	223
Chapter Review	224
Key Terms	224
Case Scenarios	224
Case Scenario 1: Creating Computer Objects and Joining the Domain	225
Case Scenario 2: Automating the Creation of Computer Objects	225
Suggested Practices	225
Create and Maintain Computer Accounts	225
Take a Practice Test	227
6 Group Policy Infrastructure	229
Before You Begin	230
Lesson 1: Implementing Group Policy	231
An Overview and Review of Group Policy	231
Group Policy Objects	237
Policy Settings	241

Administrative Templates Node	244
Implementing Group Policy	248
Lesson Summary	252
Lesson Review	253
Lesson 2: Managing Group Policy Scope	255
GPO Links	255
GPO Inheritance and Precedence	257
Using Security Filtering to Modify GPO Scope	262
WMI Filters	264
Enabling or Disabling GPOs and GPO Nodes	266
Targeting Preferences	267
Group Policy Processing	268
Loopback Policy Processing	270
Configuring Group Policy Scope	272
Lesson Summary	275
Lesson Review	276
Lesson 3: Supporting Group Policy	277
Resultant Set of Policy	277
Examining Policy Event Logs	281
Configuring Group Policy Scope	281
Lesson Summary	284
Lesson Review	285
Chapter Review	286
Key Terms	286
Case Scenario	287
Case Scenario: Implementing Group Policy	287
Suggested Practices	287
Create and Apply Group Policy Objects (GPOs)	287
Take a Practice Test	288
7 Group Policy Settings	289
Before You Begin	289
Lesson 1: Delegating the Support of Computers	291
Understanding Restricted Groups Policies	291

Delegating Administration Using Restricted Groups Policies with the Member Of Setting	294
Delegating Membership Using Group Policy	295
Lesson Summary	298
Lesson Review	298
Lesson 2: Managing Security Settings	300
Configuring the Local Security Policy	300
Managing Security Configuration with Security Templates	302
The Security Configuration Wizard	309
Settings, Templates, Policies, and GPOs	314
Managing Security Settings	315
Lesson Summary	320
Lesson Review	321
Lesson 3: Managing Software with Group Policy Software Installation	322
Understanding Group Policy Software Installation	322
Preparing an SDP	325
Creating a Software Deployment GPO	325
Managing the Scope of a Software Deployment GPO	327
Maintaining Applications Deployed with Group Policy	327
GPSI and Slow Links	329
Managing Software with Group Policy Software Installation	329
Lesson Summary	332
Lesson Review	332
Lesson 4: Auditing	335
Audit Policy	335
Auditing Access to Files and Folders	337
Auditing Directory Service Changes	341
Auditing	342
Lesson Summary	346
Lesson Review	346
Chapter Review	348
Key Terms	349
Case Scenarios	350

Case Scenario 1: Software Installation with Group Policy Software Installation	350
Case Scenario 2: Security Configuration	350
Suggested Practices	351
Restricted Groups	351
Security Configuration	352
Take a Practice Test	354
8 Authentication.	355
Before You Begin	356
Lesson 1: Configuring Password and Lockout Policies	357
Understanding Password Policies	357
Understanding Account Lockout Policies	359
Configuring the Domain Password and Lockout Policy	360
Fine-Grained Password and Lockout Policy	360
Understanding Password Settings Objects	361
PSO Precedence and Resultant PSO	362
PSOs and OUs	362
Configuring Password and Lockout Policies	363
Lesson Summary	366
Lesson Review	367
Lesson 2: Auditing Authentication	368
Account Logon and Logon Events	368
Configuring Authentication-Related Audit Policies	369
Scoping Audit Policies	370
Viewing Logon Events	371
Auditing Authentication	371
Lesson Summary	372
Lesson Review	373
Lesson 3: Configuring Read-Only Domain Controllers	374
Authentication and Domain Controller Placement in a Branch Office	374
Read-Only Domain Controllers	375
Deploying an RODC	377
Password Replication Policy	380

Administer RODC Credentials Caching	381
Administrative Role Separation	383
Configuring Read-Only Domain Controllers	383
Lesson Summary	386
Lesson Review	387
Chapter Review	389
Key Terms	389
Case Scenarios	390
Case Scenario 1: Increasing the Security of Administrative Accounts	390
Case Scenario 2: Increasing the Security and Reliability of Branch Office Authentication	391
Suggested Practices	391
Configure Multiple Password Settings Objects	391
Recover from a Stolen Read-Only Domain Controller	392
Take a Practice Test	392
9 Integrating Domain Name System with AD DS	393
DNS and IPv6	395
The Peer Name Resolution Protocol	397
DNS Structures	398
The Split-Brain Syndrome	400
Before You Begin	403
Lesson 1: Understanding and Installing Domain Name System	406
Understanding DNS	406
Windows Server DNS Features	414
Integration with AD DS	417
Installing the DNS Service	419
Lesson Summary	429
Lesson Review	429
Lesson 2: Configuring and Using Domain Name System	431
Configuring DNS	431
Forwarders vs. Root Hints	439
Single-Label Name Management	441
DNS and DHCP Considerations	443

	Working with Application Directory Partitions	445
	Administering DNS Servers.....	448
	Finalizing a DNS Server Configuration in a Forest	450
	Lesson Summary.....	452
	Lesson Review	452
	Chapter Review.....	455
	Key Terms.....	456
	Case Scenario	456
	Case Scenario: Block Specific DNS Names.....	456
	Suggested Practices	456
	Working with DNS	456
	Take a Practice Test.....	457
10	Domain Controllers	459
	Before You Begin	459
	Lesson 1: Installing Domain Controllers	461
	Installing a Domain Controller with the Windows Interface	461
	Unattended Installation Options and Answer Files.....	462
	Installing a New Windows Server 2008 Forest.....	464
	Installing Additional Domain Controllers in a Domain.....	465
	Installing a New Windows Server 2008 Child Domain.....	467
	Installing a New Domain Tree	468
	Staging the Installation of an RODC	469
	Installing AD DS from Media	472
	Removing a Domain Controller	473
	Installing Domain Controllers	474
	Lesson Summary.....	476
	Lesson Review	477
	Lesson 2: Configuring Operations Masters	478
	Understanding Single Master Operations.....	478
	Forest-Wide Operations Master Roles.....	480
	Domain-Wide Operations Master Roles.....	480
	Placing Operations Masters	483
	Identifying Operations Masters	484

Transferring Operations Master Roles	485
Recognizing Operations Master Failures	486
Seizing Operations Master Roles	487
Returning a Role to Its Original Holder	488
Transferring Operations Master Roles	489
Lesson Summary	491
Lesson Review	492
Lesson 3: Configuring DFS Replication of SYSVOL	494
Raising the Domain Functional Level	494
Understanding Migration Stages	495
Migrating SYSVOL Replication to DFS-R	496
Configuring DFS Replication of SYSVOL	497
Lesson Summary	502
Lesson Review	502
Chapter Review	504
Key Terms	504
Case Scenario	504
Case Scenario: Upgrading a Domain	505
Suggested Practices	505
Upgrade a Windows Server 2003 Domain	505
Take a Practice Test	506
11 Sites and Replication	507
Before You Begin	508
Lesson 1: Configuring Sites and Subnets	509
Understanding Sites	509
Planning Sites	510
Defining Sites	512
Managing Domain Controllers in Sites	515
Understanding Domain Controller Location	516
Configuring Sites and Subnets	519
Lesson Summary	520
Lesson Review	521

Lesson 2: Configuring the Global Catalog and Application Directory Partitions .	522
Reviewing Active Directory Partitions	522
Understanding the Global Catalog	523
Placing GC Servers	523
Configuring a Global Catalog Server	524
Universal Group Membership Caching	524
Understanding Application Directory Partitions	525
Replication and Directory Partitions	527
Lesson Summary	529
Lesson Review	529
Lesson 3: Configuring Replication	531
Understanding Active Directory Replication	531
Connection Objects	532
The Knowledge Consistency Checker	533
Intrasite Replication	534
Site Links	535
Bridgehead Servers	538
Configuring Intersite Replication	539
Monitoring Replication	543
Configuring Replication	545
Lesson Summary	547
Lesson Review	547
Chapter Review	550
Key Terms	551
Case Scenario	551
Case Scenario: Configuring Sites and Subnets	551
Suggested Practices	553
Monitor and Manage Replication	553
Take a Practice Test	554
12 Domains and Forests	555
Before You Begin	555
Lesson 1: Understanding Domain and Forest Functional Levels	557
Understanding Functional Levels	557

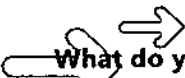
Domain Functional Levels	557
Forest Functional Levels	560
Raising the Domain and Forest Functional Levels	563
Lesson Summary	565
Lesson Review	565
Lesson 2: Managing Multiple Domains and Trust Relationships	567
Defining Your Forest and Domain Structure	567
Moving Objects Between Domains and Forests	572
Understanding Trust Relationships	576
Authentication Protocols and Trust Relationships	579
Manual Trusts	583
Administering Trusts	590
Securing Trust Relationships	591
Administering a Trust Relationship	595
Lesson Summary	601
Lesson Review	602
Chapter Review	604
Chapter Summary	604
Case Scenario	605
Case Scenario: Managing Multiple Domains and Forests	605
Suggested Practices	605
Configure a Forest or Domain	605
Take a Practice Test	606
13 Directory Business Continuity	607
Before You Begin	608
Lesson 1: Proactive Directory Maintenance and Data Store Protection	610
Twelve Categories of AD DS Administration	612
Performing Online Maintenance	622
Performing Offline Maintenance	623
Relying on Built-in Directory Protection Measures	624
Relying on Windows Server Backup to Protect the Directory	629
Performing Proactive Restores	638
Protecting DCs as Virtual Machines	648

	Working with the AD DS Database	650
	Lesson Summary	657
	Lesson Review	658
	Lesson 2: Proactive Directory Performance Management	660
	Managing System Resources	660
	Working with Windows System Resource Manager	672
	AD DS Performance Analysis	675
	Lesson Summary	680
	Lesson Review	680
	Chapter Review	682
	Key Terms	683
	Case Scenario	683
	Case Scenario: Working with Lost and Found Data	683
	Suggested Practices	684
	Proactive Directory Maintenance	684
	Take a Practice Test	684
14	Active Directory Lightweight Directory Services	685
	Before You Begin	687
	Lesson 1: Understanding and Installing AD LDS	690
	Understanding AD LDS	690
	AD LDS Scenarios	692
	Installing AD LDS	694
	Installing AD LDS	696
	Lesson Summary	699
	Lesson Review	699
	Lesson 2: Configuring and Using AD LDS	701
	Working with AD LDS Tools	701
	Creating AD LDS Instances	703
	Working with AD LDS Instances	709
	Working with AD LDS Instances	714
	Lesson Summary	718
	Lesson Review	719
	Chapter Review	720

Chapter Summary	720
Key Terms	721
Case Scenario	721
Case Scenario: Determine AD LDS Instance Prerequisites	721
Suggested Practices	721
Work with AD LDS Instances	722
Take a Practice Test	722
15 Active Directory Certificate Services and Public Key Infrastructures. .	723
Before You Begin	727
Lesson 1: Understanding and Installing Active Directory Certificate Services ...	730
Understanding AD CS	731
Installing AD CS	740
Installing a CA Hierarchy	742
Lesson Summary	750
Lesson Review	751
Lesson 2: Configuring and Using Active Directory Certificate Services	753
Finalizing the Configuration of an Issuing CA	753
Finalizing the Configuration of an Online Responder	759
Considerations for the Use and Management of AD CS	763
Working with Enterprise PKI	765
Protecting Your AD CS Configuration	766
Configuring and Using AD CS	767
Lesson Summary	773
Lesson Review	774
Chapter Review	776
Key Terms	777
Case Scenario	777
Case Scenario: Manage Certificate Revocation	777
Suggested Practices	778
Working with AD CS	778
Take a Practice Test	779

16	Active Directory Rights Management Services	781
	Before You Begin	784
	Lesson 1: Understanding and Installing Active Directory Rights Management Services	786
	Understanding AD RMS	786
	Installing Active Directory Rights Management Services	794
	Installing AD RMS	802
	Lesson Summary	807
	Lesson Review	808
	Lesson 2: Configuring and Using Active Directory Rights Management Services	809
	Configuring AD RMS	810
	Creating a Rights Policy Template	819
	Lesson Summary	820
	Lesson Review	821
	Chapter Review	822
	Key Terms	823
	Case Scenario	823
	Case Scenario: Prepare to Work with an External AD RMS Cluster	823
	Suggested Practices	823
	Work with AD RMS	824
	Take a Practice Test	824
17	Active Directory Federation Services	825
	The Purpose of a Firewall	826
	Active Directory Federation Services	827
	Before You Begin	829
	Lesson 1: Understanding Active Directory Federation Services	832
	The AD FS Authentication Process	833
	Working with AD FS Designs	836
	Understanding AD FS Components	838
	Installing Active Directory Federation Services	845
	Prepare an AD FS Deployment	849

Lesson Summary	852
Lesson Review	853
Lesson 2: Configuring and Using Active Directory Federation Services	854
Finalize the Configuration of AD FS	854
Using and Managing AD FS	855
Finalizing the AD FS Configuration	857
Lesson Summary	869
Lesson Review	870
Chapter Review	871
Key Terms	872
Case Scenario	872
Case Scenario: Choose the Right AD Technology	872
Suggested Practices	873
Prepare for AD FS	873
Take a Practice Test	873
Answers	875
Index	921

 **What do you think of this book? We want to hear from you!**

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

Heartfelt Thanks

Nelson, Danielle, Tony, and I would like to pay tribute to the incredible folks at Microsoft Press for giving us the opportunity to contribute to the Windows Server 2008 training and certification effort. Starting with Laura Sackerman and Ken Jones: you pulled us together in 2007 and created a framework that was both comfortable and effective, bringing out the best in us as authors and resulting in what we believe is a tremendous resource for the Windows IT professional community. Thanks for giving us the chance to write about a technology we love! Maureen Zimmerman, your tireless attention to detail and nurturing of the process brought us, and this training kit, across a finish line that at times seemed elusive. I know I owe you special thanks for your faith in me and your support and “props” along the way. Bob Hogan, you kept us honest and contributed great ideas to the cause. Kerin Forsyth, you make us sound better than we really are. Bob Dean, we all are grateful that with your efforts, the practice test questions for this training kit are first class. And Chris Norton, without you, there wouldn't be a page to look at, let alone hundreds of pages of valuable training and reference. Thanks to all of you, from all of us!

Finally, my own deepest gratitude goes to my Einstein, and we all thank our families, our friends, and our muses who make it possible and worthwhile.

Introduction

This training kit is designed for IT professionals who support or plan to support Microsoft Windows Server 2008 Active Directory Domain Services (AD DS) and who also plan to take the Microsoft Certified Technology Specialist (MCTS) 70-640 examination. It is assumed that, before you begin using this kit, you have a solid foundation-level understanding of Microsoft Windows client and server operating systems and common Internet technologies. The MCTS exam, and this book, assume that you have at least one year of experience administering AD DS.

The material covered in this training kit and on the 70-640 exam builds on your understanding and experience to help you implement AD DS in distributed environments that can include complex network services and multiple locations and domain controllers. By using this training kit, you will learn how to do the following:

- Deploy Active Directory Domain Services, Active Directory Lightweight Directory Services, Active Directory Certificate Services, Active Directory Federation Services, and Active Directory Rights Management Services in a forest or domain.
- Upgrade existing domain controllers, domains, and forests to Windows Server 2008.
- Efficiently administer and automate the administration of users, groups, and computers.
- Manage the configuration and security of a domain by using Group Policy, fine-grained password policies, directory services auditing, and the Security Configuration Wizard.
- Implement effective name resolution with Domain Name System (DNS) on Windows Server 2008.
- Plan, configure, and support the replication of Active Directory data within and between sites.
- Add, remove, maintain, and back up domain controllers.
- Enable authentication between domains and forests.
- Implement new capabilities and functionality offered by Windows Server 2008.

Find additional content online As new or updated material that complements your book becomes available, it will be posted on the Microsoft Press Online Windows Server and Client Web site. Based on the final build of Windows Server 2008, the type of material you might find includes updates to book content, articles, links to companion content, errata, sample chapters, and more. This Web site will be available soon at <http://www.microsoft.com/learning/books/online/serverclient> and will be updated periodically.

Making the Most of the Training Kit

This training kit will prepare you for the 70-640 MCTS exam, which covers a large number of concepts and skills related to the implementation and administration of AD DS on Windows Server 2008. To provide you with the best possible learning experience, each lesson in the training kit includes content, practices, and review questions, and each chapter adds case scenario exercises and suggested practices. The companion CD provides links to external resources and dozens of sample questions.

We recommend that you take advantage of each of these components in the training kit. Some concepts or skills are easiest to learn within the context of a practice or sample questions, so these concepts and skills might be introduced in the practices or sample questions and not in the main body of the lesson. Don't make the mistake of reading the lessons and not performing the practices or of performing practices and taking sample exams without reading the lessons. Even if you do not have an environment with which to perform practices, at least read and think through the steps so that you gain the benefit of the new ideas they introduce.

Setup and Hardware Requirements

Practice exercises are a valuable component of this training kit. They enable you to experience important skills directly, reinforce material discussed in lessons, and even introduce new concepts. Each lesson and practice describes the requirements for exercises. Although many lessons require only one computer, configured as a domain controller for a sample domain named *contoso.com*, some lessons require additional computers acting as a second domain controller in the domain, as a domain controller in another domain in the same forest, as a domain controller in another forest, or as a server performing other roles.

The chapters that cover AD DS (chapters 1–13) require, at most, three machines running simultaneously. Chapters covering other Active Directory roles require up to seven machines running simultaneously to provide a comprehensive experience with the technology.

It is highly recommended that you use virtual machines rather than physical computers to work through the lessons and practices. Doing so will reduce the time and expense of configuring physical computers. You can use Virtual PC 2007 or later or Virtual Server 2005 R2 or later, which you can download for free at <http://www.microsoft.com/downloads>. You can use other virtualization software instead, such as VMware Workstation or VMware Server, which can be downloaded at <http://www.vmware.com>. Refer to the documentation of your selected virtualization software for guidance regarding the creation of virtual machines for Windows Server 2008.

Windows Server 2008 can run comfortably with 512 megabytes (MB) of memory in small environments such as the sample *contoso.com* domain. As you provision virtual machines, be sure to give each machine at least 512 MB of RAM. It is recommended that the physical host

running the virtual machines have sufficient physical RAM for the host operating system and each of the concurrently running virtual machines. If you encounter performance bottlenecks while running multiple virtual machines on a single physical host, consider running virtual machines on different physical hosts. Ensure that all virtual machines can network with each other. It is highly recommended that the environment be totally disconnected from your production environment.

The authors recommend that you preserve each of the virtual machines you create until you have completed the training kit. After each chapter, create a backup or snapshot of the virtual machines used in that chapter so that you can reuse them as required in later exercises.

Software Requirements and Setup

You must have a copy of Windows Server 2008 to perform the exercises in this training kit. Several exercises require Windows Server 2003, and some optional exercises require Windows Vista.

Evaluation versions of Windows Server 2008 can be downloaded from <http://www.microsoft.com/downloads>. To perform the exercises in this training kit, you can install either the Standard or Enterprise editions, and you can use either 32-bit or 64-bit versions, according to the hardware or virtualization platform you have selected. Chapter 1, "Installation," includes setup instructions for the first domain controller in the *contoso.com* domain, which is used throughout this training kit. Lessons that require an additional computer provide guidance regarding the configuration of that computer.

Using the CD

A companion CD, included with this training kit, contains the following:

- **Practice tests** You can reinforce your understanding of how to configure Windows Server 2008 by using electronic practice tests you customize to meet your needs from the pool of Lesson Review questions in this book. Alternatively, you can practice for the 70-640 certification exam by using tests created from a pool of 200 realistic exam questions, which give you many practice scenarios to ensure that you are prepared.
- **An eBook** An electronic version (eBook) of this book is included for when you do not want to carry the printed book with you. The eBook is in Portable Document Format (PDF), and you can view it by using Adobe Acrobat or Adobe Reader.
- **Sample chapters** Sample chapters from other Microsoft Press titles on Windows Server 2008 are offered on the CD. These chapters are in PDF.

Digital Content for Digital Book Readers: If you bought a digital-only edition of this book, you can enjoy select content from the print edition's companion CD. Visit <http://go.microsoft.com/fwlink/?LinkId=114977> to get your downloadable content. This content is always up-to-date and available to all readers.

How to Install the Practice Tests

To install the practice test software from the companion CD to your hard disk, do the following:

1. Insert the companion CD into your CD drive and accept the license agreement. A CD menu appears.

NOTE If the CD menu does not appear

If the CD menu or the license agreement does not appear, AutoRun might be disabled on your computer. Refer to the Readme.txt file on the CD-ROM for alternate installation instructions.

2. Click Practice Tests and follow the instructions on the screen.

How to Use the Practice Tests

To start the practice test software, follow these steps.

1. Click Start\All Programs\Microsoft Press Training Kit Exam Prep.
A window appears that shows all the Microsoft Press training kit exam prep suites installed on your computer.
2. Double-click the lesson review or practice test you want to use.

NOTE Lesson reviews vs. practice tests

Select the (70-640) TS: Configuring Windows Server 2008 Active Directory *lesson review* to use the questions from the "Lesson Review" sections of this book. Select the (70-640) TS: Configuring Windows Server 2008 Active Directory *practice test* to use a pool of 200 questions similar to those that appear on the 70-640 certification exam.

Lesson Review Options

When you start a lesson review, the Custom Mode dialog box appears so that you can configure your test. You can click OK to accept the defaults, or you can customize the number of questions you want, how the practice test software works, which exam objectives you want the questions to relate to, and whether you want your lesson review to be timed. If you are retaking a test, you can select whether you want to see all the questions again or only the questions you missed or did not answer.

After you click OK, your lesson review starts.

- To take the test, answer the questions and use the Next and Previous buttons to move from question to question.
- After you answer an individual question, if you want to see which answers are correct—along with an explanation of each correct answer—click Explanation.
- If you prefer to wait until the end of the test to see how you did, answer all the questions and then click Score Test. You will see a summary of the exam objectives you chose and the percentage of questions you got right overall and per objective. You can print a copy of your test, review your answers, or retake the test.

Practice Test Options

When you start a practice test, you choose whether to take the test in Certification Mode, Study Mode, or Custom Mode.

- **Certification Mode** Closely resembles the experience of taking a certification exam. The test has a set number of questions. It is timed, and you cannot pause and restart the timer.
- **Study Mode** Creates an untimed test in which you can review the correct answers and the explanations after you answer each question.
- **Custom Mode** Gives you full control over the test options so that you can customize them as you like.

In all modes, the user interface when you are taking the test is basically the same but with different options enabled or disabled, depending on the mode. The main options are discussed in the previous section, “Lesson Review Options.”

When you review your answer to an individual practice test question, a “References” section is provided that lists where in the training kit you can find the information that relates to that question and provides links to other sources of information. After you click Test Results to score your entire practice test, you can click the Learning Plan tab to see a list of references for every objective.

How to Uninstall the Practice Tests

To uninstall the practice test software for a training kit, use the Add Or Remove Programs option (Windows XP) or the Programs And Features option (Windows Vista) in Windows Control Panel.

Microsoft Certified Professional Program

The Microsoft certifications provide the best method to prove your command of current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop or implement and support solutions with Microsoft products and technologies. Computer professionals who become Microsoft certified are recognized as experts and are sought after industry-wide. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO All the Microsoft certifications

For a full list of Microsoft certifications, go to <http://www.microsoft.com/learning/mcp/default.asp>.

Technical Support

Every effort has been made to ensure the accuracy of this book and the contents of the companion CD. If you have comments, questions, or ideas regarding this book or the companion CD, please send them to Microsoft Press by using either of the following methods:

- E-mail: tkinput@microsoft.com
- Postal mail at:

Microsoft Press

Attn: *MCTS Self-Paced Training Kit (Exam 70-640): Configuring Windows Server 2008*

Active Directory, Editor

One Microsoft Way

Redmond, WA 98052-6399

For additional support information regarding this book and the CD-ROM (including answers to commonly asked questions about installation and use), visit the Microsoft Press Book and CD Support Web site at <http://www.microsoft.com/learning/support/books>. To connect directly to Microsoft Knowledge Base and enter a query, visit <http://support.microsoft.com/search>. For support information regarding Microsoft software, connect to <http://support.microsoft.com>.