

*Solutions for Administrators  
& Developers*

**3rd Edition**  
Covers Windows 2008,  
Exchange 2007, and PowerShell



# Active Directory Cookbook™

O'REILLY®

*Laura E. Hunter  
& Robbie Allen*

## Active Directory Cookbook



When you need practical, hands-on support for Active Directory, this updated edition provides quick solutions to more than 300 common (and not so common) problems you might encounter when deploying, administering, and automating Microsoft's network directory service.

For this third edition, Active Directory expert Laura E. Hunter offers troubleshooting recipes based on valuable input from Windows administrators, in addition to her own experience. You'll find solutions for problems with the Lightweight Directory Access Protocol (LDAP), ADAM (Active Directory Application Mode), multi-master replication, Domain Name System (DNS), Group Policy, the Active Directory Schema, and many other features.

With *Active Directory Cookbook*, you will:

- Perform Active Directory tasks from the command line
- Use scripting technologies to automate Active Directory tasks
- Manage new Active Directory features, such as Read-Only Domain Controllers, Fine-Grained Password Policies, and more
- Create domains and trusts
- Apply a security filter to Group Policy Objects
- Check for potential replication problems
- Restrict hosts from performing LDAP queries
- View DNS server performance statistics

Each recipe includes a discussion explaining how and why the solution works, so you can adapt the techniques to your own situations.

[www.oreilly.com](http://www.oreilly.com)

US \$59.99

CAN \$59.99

ISBN: 978-0-596-52110-3



5 5 9 9 9

**Safari**<sup>®</sup>  
Books Online

Free online edition  
for 45 days with  
purchase of this book.  
Details on last page.

---

*"If you already understand Active Directory fundamentals and are looking for a quick solution to common Active Directory related tasks, look no further, you have found the book that you need."*

—Joe Richards,  
Directory Services MVP

---

*"The Active Directory Cookbook is the real deal...a soup-to-nuts catalog of every administrative task an Active Directory administrator needs to perform."*

—Gil Kirkpatrick, Chief  
Architect, Active  
Directory and Identity  
Management, Quest  
Software and Directory  
Services MVP

---

Laura E. Hunter is an identity architect with the Oxford Computer Group.

Robbie Allen is an author, entrepreneur, web industry veteran, and founder of the popular sports website Statsheet.com.

---

THIRD EDITION

---

# Active Directory Cookbook™

*Laura E. Hunter and Robbie Allen*

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Sebastopol • Taipei • Tokyo

---

**Active Directory Cookbook<sup>™</sup>, Third Edition**

by Laura E. Hunter and Robbie Allen

Copyright © 2009 O'Reilly Media. All rights reserved.  
Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (<http://safari.oreilly.com>). For more information, contact our corporate/institutional sales department: (800) 998-9938 or [corporate@oreilly.com](mailto:corporate@oreilly.com).

**Editors:** John Osborn and Laurel R.T. Ruma

**Production Editor:** Loranah Dimant

**Copyeditor:** Colleen Gorman

**Proofreader:** Sada Preisch

**Indexer:** Ellen Troutman Zaig

**Cover Designer:** Karen Montgomery

**Interior Designer:** David Futato

**Illustrator:** Jessamyn Read

**Printing History:**

September 2003: First Edition.

June 2006: Second Edition.

December 2008: Third Edition.

Nutshell Handbook, the Nutshell Handbook logo, and the O'Reilly logo are registered trademarks of O'Reilly Media, Inc. *Active Directory Cookbook*, the image of a bluefin tuna, and related trade dress are trademarks of O'Reilly Media, Inc.

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and O'Reilly Media, Inc., was aware of a trademark claim, the designations have been printed in caps or initial caps.

While every precaution has been taken in the preparation of this book, the publisher and authors assume no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

ISBN: 978-0-596-52110-3

[M]

1229006171

---

# Table of Contents

<b>Preface .....</b>	<b>xvii</b>
<b>1. Getting Started .....</b>	<b>1</b>
1.1 Approach to the Book	1
1.2 Where to Find the Tools	3
1.3 Getting Familiar with LDIF	5
1.4 Programming Notes	7
1.5 Replaceable Text	10
1.6 Where to Find More Information	11
<b>2. Forests, Domains, and Trusts .....</b>	<b>15</b>
2.1 Creating a Forest	21
2.2 Removing a Forest	22
2.3 Creating a Domain	24
2.4 Removing a Domain	25
2.5 Removing an Orphaned Domain	27
2.6 Finding the Domains in a Forest	28
2.7 Finding the NetBIOS Name of a Domain	30
2.8 Renaming a Domain	32
2.9 Raising the Domain Mode to Windows 2000 Native Mode	33
2.10 Viewing and Raising the Functional Level of a Windows Server 2003 or 2008 Domain	36
2.11 Raising the Functional Level of a Windows Server 2003 or 2008 Forest	39
2.12 Using AdPrep to Prepare a Domain or Forest for Windows Server 2003 or 2008	42
2.13 Determining Whether AdPrep Has Completed	44
2.14 Checking If a Windows Domain Controller Can Be Upgraded to Windows Server 2003 or 2008	47
2.15 Creating an External Trust	48
2.16 Creating a Transitive Trust Between Two AD Forests	50
2.17 Creating a Shortcut Trust Between Two AD Domains	52

2.18	Creating a Trust to a Kerberos Realm	53
2.19	Viewing the Trusts for a Domain	55
2.20	Verifying a Trust	58
2.21	Resetting a Trust	60
2.22	Removing a Trust	62
2.23	Enabling SID Filtering for a Trust	64
2.24	Enabling Quarantine for a Trust	66
2.25	Managing Selective Authentication for a Trust	66
2.26	Finding Duplicate SIDs in a Domain	69
2.27	Adding Additional Fields to Active Directory Users and Computers	70
<b>3.</b>	<b>Domain Controllers, Global Catalogs, and FSMOs</b>	<b>73</b>
3.1	Promoting a Domain Controller	76
3.2	Promoting a Read-Only Domain Controller	77
3.3	Performing a Two-Stage RODC Installation	78
3.4	Modifying the Password Replication Policy	80
3.5	Promoting a Windows Server 2003 Domain Controller from Media	82
3.6	Promoting a Windows Server 2008 Domain Controller from Media	84
3.7	Demoting a Domain Controller	86
3.8	Automating the Promotion or Demotion of a Domain Controller	87
3.9	Troubleshooting Domain Controller Promotion or Demotion Problems	88
3.10	Verifying the Promotion of a Domain Controller	89
3.11	Removing an Unsuccessfully Demoted Domain Controller	90
3.12	Renaming a Domain Controller	93
3.13	Finding the Domain Controllers for a Domain	95
3.14	Finding the Closest Domain Controller	96
3.15	Finding a Domain Controller's Site	98
3.16	Moving a Domain Controller to a Different Site	101
3.17	Finding the Services a Domain Controller Is Advertising	104
3.18	Restoring a Deleted Domain Controller	105
3.19	Resetting the TCP/IP Stack on a Domain Controller	106
3.20	Configuring a Domain Controller to Use an External Time Source	107
3.21	Finding the Number of Logon Attempts Made Against a Domain Controller	110
3.22	Enabling the /3GB Switch to Increase the LSASS Cache	110
3.23	Cleaning Up Distributed Link Tracking Objects	112
3.24	Enabling and Disabling the Global Catalog	113
3.25	Determining Whether Global Catalog Promotion Is Complete	115
3.26	Finding the Global Catalog Servers in a Forest	117
3.27	Finding the Domain Controllers or Global Catalog Servers in a Site	119

3.28	Finding Domain Controllers and Global Catalogs via DNS	121
3.29	Changing the Preference for a Domain Controller	122
3.30	Disabling the Global Catalog Requirement During a Domain Login	124
3.31	Disabling the Global Catalog Requirement for Windows Server 2003 or Windows Server 2008	125
3.32	Finding the FSMO Role Holders	126
3.33	Transferring a FSMO Role	129
3.34	Seizing a FSMO Role	131
3.35	Finding the PDC Emulator FSMO Role Owner via DNS	132
3.36	Finding the PDC Emulator FSMO Role Owner via WINS	133
<b>4.</b>	<b>Searching and Manipulating Objects</b>	<b>135</b>
4.1	Viewing the RootDSE	136
4.2	Viewing the Attributes of an Object	140
4.3	Counting Objects in Active Directory	145
4.4	Using LDAP Controls	147
4.5	Using a Fast or Concurrent Bind	150
4.6	Connecting to an Object GUID	152
4.7	Connecting to a Well-Known GUID	153
4.8	Searching for Objects in a Domain	155
4.9	Searching the Global Catalog	158
4.10	Searching for a Large Number of Objects	161
4.11	Searching with an Attribute-Scoped Query	164
4.12	Searching with a Bitwise Filter	166
4.13	Creating an Object	170
4.14	Modifying an Object	173
4.15	Modifying a Bit Flag Attribute	177
4.16	Dynamically Linking an Auxiliary Class	180
4.17	Creating a Dynamic Object	182
4.18	Refreshing a Dynamic Object	184
4.19	Modifying the Default TTL Settings for Dynamic Objects	186
4.20	Moving an Object to a Different OU or Container	188
4.21	Moving an Object to a Different Domain	191
4.22	Referencing an External Domain	193
4.23	Renaming an Object	195
4.24	Deleting an Object	197
4.25	Deleting a Container That Has Child Objects	200
4.26	Viewing the Created and Last Modified Timestamp of an Object	202
4.27	Modifying the Default LDAP Query Policy	203
4.28	Exporting Objects to an LDIF File	206
4.29	Importing Objects Using an LDIF File	207
4.30	Exporting Objects to a CSV File	208

---

4.31	Importing Objects Using a CSV File	209
<b>5.</b>	<b>Organizational Units</b>	<b>211</b>
5.1	Creating an OU	212
5.2	Enumerating the OUs in a Domain	214
5.3	Finding an OU	216
5.4	Enumerating the Objects in an OU	218
5.5	Deleting the Objects in an OU	221
5.6	Deleting an OU	222
5.7	Moving the Objects in an OU to a Different OU	223
5.8	Moving an OU	226
5.9	Renaming an OU	227
5.10	Modifying an OU	229
5.11	Determining Approximately How Many Child Objects an OU Has	231
5.12	Delegating Control of an OU	233
5.13	Assigning or Removing a Manager for an OU	234
5.14	Linking a GPO to an OU	235
5.15	Protecting an OU Against Accidental Deletion	238
<b>6.</b>	<b>Users</b>	<b>241</b>
6.1	Modifying the Default Display Name Used When Creating Users in ADUC	244
6.2	Creating a User	245
6.3	Creating a Large Number of Users	248
6.4	Creating an inetOrgPerson User	250
6.5	Converting a user Object to an inetOrgPerson Object (or Vice Versa)	253
6.6	Modifying an Attribute for Several Users at Once	255
6.7	Deleting a User	256
6.8	Setting a User's Profile Attributes	258
6.9	Moving a User	260
6.10	Redirecting Users to an Alternative OU	261
6.11	Renaming a User	263
6.12	Copying a User	265
6.13	Finding Locked-Out Users	267
6.14	Unlocking a User	268
6.15	Troubleshooting Account Lockout Problems	270
6.16	Viewing the Domain-Wide Account Lockout and Password Policies	271
6.17	Applying a Fine-Grained Password Policy to a User Object	275
6.18	Viewing the Fine-Grained Password Policy That Is in Effect for a User Account	276
6.19	Enabling and Disabling a User	278



6.20	Finding Disabled Users	279
6.21	Viewing a User's Group Membership	281
6.22	Removing All Group Memberships from a User	284
6.23	Changing a User's Primary Group	285
6.24	Copying a User's Group Membership to Another User	287
6.25	Setting a User's Password	290
6.26	Preventing a User from Changing a Password	291
6.27	Requiring a User to Change a Password at Next Logon	293
6.28	Preventing a User's Password from Expiring	294
6.29	Finding Users Whose Passwords Are About to Expire	296
6.30	Viewing the RODCs That Have Cached a User's Password	297
6.31	Setting a User's Account Options (userAccountControl)	299
6.32	Setting a User's Account to Expire	302
6.33	Determining a User's Last Logon Time	303
6.34	Finding Users Who Have Not Logged On Recently	306
6.35	Viewing and Modifying a User's Permitted Logon Hours	307
6.36	Viewing a User's Managed Objects	309
6.37	Creating a UPN Suffix for a Forest	311
6.38	Restoring a Deleted User	312
6.39	Protecting a User Against Accidental Deletion	313
<b>7.</b>	<b>Groups</b>	<b>315</b>
7.1	Creating a Group	316
7.2	Viewing the Permissions of a Group	319
7.3	Viewing the Direct Members of a Group	322
7.4	Viewing the Nested Members of a Group	324
7.5	Adding and Removing Members of a Group	326
7.6	Moving a Group Within a Domain	328
7.7	Moving a Group to Another Domain	330
7.8	Changing the Scope or Type of a Group	332
7.9	Modifying Group Attributes	334
7.10	Creating a Dynamic Group	337
7.11	Delegating Control for Managing Membership of a Group	339
7.12	Resolving a Primary Group ID	342
7.13	Enabling Universal Group Membership Caching	344
7.14	Restoring a Deleted Group	347
7.15	Protecting a Group Against Accidental Deletion	348
7.16	Applying a Fine-Grained Password Policy to a Group Object	349
<b>8.</b>	<b>Computer Objects</b>	<b>351</b>
8.1	The Anatomy of a computer Object	351
8.2	Creating a Computer	352
8.3	Creating a Computer for a Specific User or Group	354

8.4	Deleting a Computer	360
8.5	Joining a Computer to a Domain	361
8.6	Moving a Computer Within the Same Domain	364
8.7	Moving a Computer to a New Domain	365
8.8	Renaming a Computer	367
8.9	Adding or Removing a Computer Account from a Group	370
8.10	Testing the Secure Channel for a Computer	371
8.11	Resetting a Computer Account	372
8.12	Finding Inactive or Unused Computers	374
8.13	Changing the Maximum Number of Computers a User Can Join to the Domain	375
8.14	Modifying the Attributes of a computer Object	377
8.15	Finding Computers with a Particular OS	379
8.16	Binding to the Default Container for Computers	382
8.17	Changing the Default Container for Computers	385
8.18	Listing All the Computer Accounts in a Domain	387
8.19	Identifying a Computer Role	388
8.20	Protecting a Computer Against Accidental Deletion	390
8.21	Viewing the RODCs That Have Cached a Computer's Password	391
<b>9.</b>	<b>Group Policy Objects .....</b>	<b>393</b>
9.1	Finding the GPOs in a Domain	396
9.2	Creating a GPO	397
9.3	Copying a GPO	399
9.4	Deleting a GPO	402
9.5	Viewing the Settings of a GPO	403
9.6	Modifying the Settings of a GPO	406
9.7	Importing Settings into a GPO	407
9.8	Creating a Migration Table	410
9.9	Creating Custom Group Policy Settings	412
9.10	Assigning Logon/Logoff and Startup/Shutdown Scripts in a GPO	415
9.11	Installing Applications with a GPO	416
9.12	Disabling the User or Computer Settings in a GPO	417
9.13	Listing the Links for a GPO	419
9.14	Creating a GPO Link to an OU	422
9.15	Blocking Inheritance of GPOs on an OU	424
9.16	Enforcing the Settings of a GPO Link	426
9.17	Applying a Security Filter to a GPO	428
9.18	Delegating Administration of GPOs	431
9.19	Importing a Security Template	433
9.20	Creating a WMI Filter	434
9.21	Applying a WMI Filter to a GPO	436
9.22	Configuring Loopback Processing for a GPO	438

9.23	Backing Up a GPO	439
9.24	Restoring a GPO	442
9.25	Simulating the RSoP	445
9.26	Viewing the RSoP	446
9.27	Refreshing GPO Settings on a Computer	447
9.28	Restoring a Default GPO	448
9.29	Creating a Fine-Grained Password Policy	449
9.30	Editing a Fine-Grained Password Policy	452
9.31	Viewing the Effective PSO for a User	454
<b>10.</b>	<b>Schema .....</b>	<b>457</b>
10.1	Registering the Active Directory Schema MMC Snap-in	459
10.2	Enabling Schema Updates	460
10.3	Generating an OID to Use for a New Class or Attribute	462
10.4	Extending the Schema	463
10.5	Preparing the Schema for an Active Directory Upgrade	464
10.6	Documenting Schema Extensions	465
10.7	Adding a New Attribute	466
10.8	Viewing an Attribute	470
10.9	Adding a New Class	473
10.10	Viewing a Class	475
10.11	Indexing an Attribute	476
10.12	Modifying the Attributes That Are Copied When Duplicating a User	479
10.13	Adding Custom Information to ADUC	481
10.14	Modifying the Attributes Included with ANR	483
10.15	Modifying the Set of Attributes Stored on a Global Catalog	486
10.16	Finding Nonreplicated and Constructed Attributes	489
10.17	Finding the Linked Attributes	492
10.18	Finding the Structural, Auxiliary, Abstract, and 88 Classes	494
10.19	Finding the Mandatory and Optional Attributes of a Class	497
10.20	Modifying the Default Security of a Class	499
10.21	Managing the Confidentiality Bit	501
10.22	Adding an Attribute to the Read-Only Filtered Attribute Set (RO-FAS)	503
10.23	Deactivating Classes and Attributes	505
10.24	Redefining Classes and Attributes	507
10.25	Reloading the Schema Cache	507
10.26	Managing the Schema Master FSMO	509
<b>11.</b>	<b>Site Topology .....</b>	<b>513</b>
11.1	Creating a Site	517
11.2	Listing Sites in a Forest	519
11.3	Renaming a Site	521

11.4	Deleting a Site	522
11.5	Delegating Control of a Site	523
11.6	Configuring Universal Group Caching for a Site	526
11.7	Creating a Subnet	528
11.8	Listing the Subnets	530
11.9	Finding Missing Subnets	531
11.10	Deleting a Subnet	534
11.11	Changing a Subnet's Site Assignment	535
11.12	Creating a Site Link	537
11.13	Finding the Site Links for a Site	539
11.14	Modifying the Sites That Are Part of a Site Link	541
11.15	Modifying the Cost for a Site Link	543
11.16	Enabling Change Notification for a Site Link	545
11.17	Modifying Replication Schedules	547
11.18	Disabling Site Link Transitivity or Site Link Schedules	549
11.19	Creating a Site Link Bridge	551
11.20	Finding the Bridgehead Servers for a Site	553
11.21	Setting a Preferred Bridgehead Server for a Site	554
11.22	Listing the Servers	556
11.23	Moving a Domain Controller to a Different Site	558
11.24	Configuring a Domain Controller to Cover Multiple Sites	560
11.25	Viewing the Site Coverage for a Domain Controller	561
11.26	Disabling Automatic Site Coverage for a Domain Controller	562
11.27	Finding the Site for a Client	563
11.28	Forcing a Host into a Particular Site	564
11.29	Creating a Connection Object	565
11.30	Listing the connection Objects for a Server	566
11.31	Load-Balancing connection Objects	568
11.32	Finding the ISTG for a Site	568
11.33	Transferring the ISTG to Another Server	570
11.34	Triggering the KCC	572
11.35	Determining Whether the KCC Is Completing Successfully	573
11.36	Disabling the KCC for a Site	574
11.37	Changing the Interval at Which the KCC Runs	577
<b>12.</b>	<b>Replication .....</b>	<b>579</b>
12.1	Determining Whether Two Domain Controllers Are in Sync	579
12.2	Viewing the Replication Status of Several Domain Controllers	582
12.3	Viewing Unreplicated Changes Between Two Domain Controllers	583
12.4	Forcing Replication from One Domain Controller to Another	586
12.5	Enabling and Disabling Replication	588
12.6	Changing the Intra-Site Replication Interval	589

12.7	Changing the Intra-Site Notification Delay	590
12.8	Changing the Inter-Site Replication Interval	593
12.9	Disabling Inter-Site Compression of Replication Traffic	595
12.10	Checking for Potential Replication Problems	597
12.11	Enabling Enhanced Logging of Replication Events	597
12.12	Enabling Strict or Loose Replication Consistency	597
12.13	Finding Conflict Objects	599
12.14	Finding Orphaned Objects	602
12.15	Listing the Replication Partners for a DC	604
12.16	Viewing Object Metadata	605
<b>13.</b>	<b>DNS and DHCP .....</b>	<b>609</b>
13.1	Creating a Forward Lookup Zone	611
13.2	Creating a Reverse Lookup Zone	613
13.3	Viewing a Server's Zones	614
13.4	Converting a Zone to an AD-Integrated Zone	617
13.5	Moving AD-Integrated Zones into an Application Partition	618
13.6	Configuring Zone Transfers	620
13.7	Configuring Forwarding	622
13.8	Delegating Control of an Active Directory Integrated Zone	625
13.9	Creating and Deleting Resource Records	627
13.10	Querying Resource Records	630
13.11	Modifying the DNS Server Configuration	631
13.12	Scavenging Old Resource Records	633
13.13	Clearing the DNS Cache	635
13.14	Verifying That a Domain Controller Can Register Its Resource Records	637
13.15	Enabling DNS Server Debug Logging	639
13.16	Registering a Domain Controller's Resource Records	642
13.17	Deregistering a Domain Controller's Resource Records	642
13.18	Preventing a Domain Controller from Dynamically Registering All Resource Records	643
13.19	Preventing a Domain Controller from Dynamically Registering Certain Resource Records	645
13.20	Allowing Computers to Use a Different Domain Suffix Than Their AD Domain	649
13.21	Authorizing a DHCP Server	651
13.22	Locating Unauthorized DHCP Servers	654
13.23	Restricting DHCP Administrators	655
<b>14.</b>	<b>Security and Authentication .....</b>	<b>659</b>
14.1	Enabling SSL/TLS	660
14.2	Encrypting LDAP Traffic with SSL, TLS, or Signing	662

14.3	Disabling LDAP Signing or Encryption	664
14.4	Enabling Anonymous LDAP Access	665
14.5	Restricting Anonymous Access to Active Directory	667
14.6	Using the Delegation of Control Wizard	669
14.7	Customizing the Delegation of Control Wizard	671
14.8	Revoking Delegated Permissions	673
14.9	Viewing the ACL for an Object	674
14.10	Customizing the ACL Editor	676
14.11	Viewing the Effective Permissions on an Object	677
14.12	Configuring Permission Inheritance	678
14.13	Changing the ACL of an Object	680
14.14	Changing the Default ACL for an Object Class in the Schema	681
14.15	Comparing the ACL of an Object to the Default Defined in the Schema	682
14.16	Resetting an Object's ACL to the Default Defined in the Schema	683
14.17	Preventing the LM Hash of a Password from Being Stored	684
14.18	Enabling Strong Domain Authentication	685
14.19	Enabling List Object Access Mode	686
14.20	Modifying the ACL on Administrator Accounts	688
14.21	Viewing and Purging Your Kerberos Tickets	689
14.22	Forcing Kerberos to Use TCP	691
14.23	Modifying Kerberos Settings	692
14.24	Viewing Access Tokens	693
<b>15.</b>	<b>Logging, Monitoring, and Quotas</b>	<b>695</b>
15.1	Enabling Extended dcpromo Logging	697
15.2	Enabling Diagnostics Logging	698
15.3	Enabling NetLogon Logging	700
15.4	Enabling GPO Client Logging	701
15.5	Enabling Kerberos Logging	704
15.6	Viewing DNS Server Performance Statistics	705
15.7	Monitoring the File Replication Service	708
15.8	Monitoring the Windows Time Service	709
15.9	Enabling Inefficient and Expensive LDAP Query Logging	710
15.10	Using the STATS Control to View LDAP Query Statistics	712
15.11	Monitoring the Performance of AD	715
15.12	Using Perfmon Trace Logs to Monitor AD	717
15.13	Creating an Administrative Alert	720
15.14	Emailing an Administrator on a Performance Alert	721
15.15	Enabling Auditing of Directory Access	723
15.16	Enabling Auditing of Registry Keys	726
15.17	Creating a Quota	727

15.18	Finding the Quotas Assigned to a Security Principal	729
15.19	Changing How Tombstone Objects Count Against Quota Usage	730
15.20	Setting the Default Quota for All Security Principals in a Partition	732
15.21	Finding the Quota Usage for a Security Principal	734
<b>16.</b>	<b>Backup, Recovery, DIT Maintenance, and Deleted Objects</b>	<b>737</b>
16.1	Backing Up Active Directory in Windows 2000 and Windows Server 2003	740
16.2	Backing Up Active Directory in Windows Server 2008	742
16.3	Creating an Active Directory Snapshot	742
16.4	Mounting an Active Directory Snapshot	743
16.5	Accessing Active Directory Snapshot Data	744
16.6	Restarting a Domain Controller in Directory Services Restore Mode	746
16.7	Resetting the Directory Service Restore Mode Administrator Password	747
16.8	Performing a Nonauthoritative Restore	749
16.9	Performing an Authoritative Restore of an Object or Subtree	750
16.10	Performing a Complete Authoritative Restore	752
16.11	Checking the DIT File's Integrity	753
16.12	Moving the DIT Files	754
16.13	Repairing or Recovering the DIT	755
16.14	Performing an Online Defrag Manually	757
16.15	Performing a Database Recovery	759
16.16	Creating a Reserve File	760
16.17	Determining How Much Whitespace Is in the DIT	761
16.18	Performing an Offline Defrag to Reclaim Space	762
16.19	Changing the Garbage Collection Interval	764
16.20	Logging the Number of Expired Tombstone Objects	766
16.21	Determining the Size of the Active Directory Database	767
16.22	Searching for Deleted Objects	769
16.23	Undeleting a Single Object	771
16.24	Undeleting a Container Object	773
16.25	Modifying the Tombstone Lifetime for a Domain	774
<b>17.</b>	<b>Application Partitions</b>	<b>777</b>
17.1	Creating and Deleting an Application Partition	779
17.2	Finding the Application Partitions in a Forest	780
17.3	Adding or Removing a Replica Server for an Application Partition	782
17.4	Finding the Replica Servers for an Application Partition	786
17.5	Finding the Application Partitions Hosted by a Server	787

17.6	Verifying Application Partitions Are Instantiated on a Server Correctly	790
17.7	Setting the Replication Notification Delay for an Application Partition	792
17.8	Setting the Reference Domain for an Application Partition	794
17.9	Delegating Control of Managing an Application Partition	796
<b>18.</b>	<b>Active Directory Application Mode and Active Directory Lightweight Directory Service</b>	<b>801</b>
18.1	Installing ADAM/AD LDS	803
18.2	Creating a New ADAM/AD LDS Instance	804
18.3	Creating a New Replica of an ADAM/AD LDS Configuration Set	806
18.4	Stopping and Starting an ADAM/AD LDS Instance	808
18.5	Changing the Ports Used by an ADAM/AD LDS Instance	810
18.6	Listing the ADAM Instances Installed on a Computer	810
18.7	Extending the ADAM/AD LDS Schema	812
18.8	Managing ADAM/AD LDS Application Partitions	813
18.9	Managing ADAM/AD LDS Organizational Units	815
18.10	Managing ADAM Users	817
18.11	Changing the Password for an ADAM or AD LDS User	819
18.12	Enabling and Disabling an ADAM User	821
18.13	Creating ADAM or AD LDS Groups	823
18.14	Managing ADAM or AD LDS Group Memberships	825
18.15	Viewing and Modifying ADAM Object Attributes	827
18.16	Importing Data into an ADAM or AD LDS Instance	829
18.17	Configuring Intra-site Replication	831
18.18	Forcing ADAM/AD LDS Replication	831
18.19	Managing AD LDS Replication Authentication	832
18.20	Managing ADAM/AD LDS Permissions	834
18.21	Enabling Auditing of AD LDS Access	836
<b>19.</b>	<b>Active Directory Federation Services</b>	<b>839</b>
19.1	Installing AD FS Prerequisites for Windows Server 2003 R2	840
19.2	Installing AD FS Prerequisites for Windows Server 2008	842
19.3	Installing the Federation Service in Windows Server 2003 R2	844
19.4	Installing the Federation Service on Windows Server 2008	846
19.5	Configuring an Active Directory Account Store	847
19.6	Configuring an ADAM or AD LDS Account Store	848
19.7	Creating Organizational Claims	849
19.8	Creating an Account Partner	851
19.9	Configuring a Resource Partner	853
19.10	Configuring an Application	854



19.11	Configuring a Forest Trust	856
19.12	Configuring an Alternate UPN Suffix	857
19.13	Configuring the AD FS Web Agent	859
19.14	Enabling Logging for the AD FS Web Agent	861
<b>20.</b>	<b>Microsoft Exchange Server 2007 and Exchange Server 2003 .....</b>	<b>863</b>
20.1	Exchange Server and Active Directory	863
20.2	Exchange Server 2007 Architecture	864
20.3	Exchange Administration Tools	864
20.4	Preparing Active Directory for Exchange	868
20.5	Installing the First Exchange Server in an Organization	873
20.6	Creating Unattended Installation Files for Exchange Server	879
20.7	Installing Exchange Management Tools	881
20.8	Stopping and Starting Exchange Server	884
20.9	Mail-Enabling a User	888
20.10	Mail-Disabling a User	894
20.11	Mailbox-Enabling a User	898
20.12	Deleting a User's Mailbox	902
20.13	Moving a Mailbox	905
20.14	Viewing Mailbox Sizes and Message Counts	910
20.15	Configuring Mailbox Limits	913
20.16	Creating an Address List	917
20.17	Creating a Storage Group	921
20.18	Creating a Mailbox Store	925
20.19	Installing Anti-Spam Agents on the Hub Transport Servers	928
20.20	Enabling Message Tracking	929
20.21	Summary	933
<b>21.</b>	<b>Microsoft Identity Lifecycle Manager .....</b>	<b>935</b>
21.1	Creating the HR Database MA	952
21.2	Creating an Active Directory MA	954
21.3	Setting Up a Metaverse Object Deletion Rule	956
21.4	Setting Up Simple Import Attribute Flow—HR Database MA	957
21.5	Setting Up a Simple Export Attribute Flow to AD	959
21.6	Defining an Advanced Import Attribute Flow—HR Database MA	960
21.7	Implementing an Advanced Attribute Flow Rules Extension—HR Database MA	962
21.8	Setting Up Advanced Export Attribute Flow in Active Directory	965
21.9	Configuring a Run Profile to Do an Initial Load of Data from the HR Database MA	967
21.10	Loading Initial HR Database Data into ILM Using a Run Profile	968

21.11	Configuring a Run Profile to Load the Container Structure from AD	969
21.12	Loading the Initial AD Container Structure into ILM Using a Run Profile	971
21.13	Setting Up the HR Database MA to Project Objects to the Metaverse	972
21.14	Writing a Rules Extension to Provision User Objects	973
21.15	Creating a Run Profile for Provisioning	976
21.16	Executing the Provisioning Rule	978
21.17	Creating a Run Profile to Export Objects from the ADMA to Active Directory	979
21.18	Exporting Objects to AD Using an Export Run Profile	980
21.19	Testing Provisioning and Deprovisioning of User Accounts in AD	982
21.20	Creating a Run Profile Script	984
21.21	Creating a Controlling Script	985
21.22	Enabling Directory Synchronization from AD to the HR Database	990
21.23	Configuring a Run Profile to Load the telephoneNumber from AD	992
21.24	Loading telephoneNumber Changes from AD into ILM Using a Delta Import and Delta Synchronization Run Profile	994
21.25	Exporting telephoneNumber Data to the HR Database	996
21.26	Using the HR Database MA Export Run Profile to Export the Telephone Number to the HR Database	997
21.27	Searching Data in the Connector Space	998
21.28	Searching Data in the Metaverse	999
21.29	Deleting Data in the Connector Space and Metaverse	1000
21.30	Extending Object Types to Include a New Attribute	1002
21.31	Previewing Changes to the ILM Configuration	1002
21.32	Committing Changes to Individual Identities Using the Commit Preview Feature	1005
21.33	Passing Data Between Rules Extensions Using Transaction Properties	1006
21.34	Using a Single Rules Extension to Affect Multiple Attribute Flows	1007
21.35	Flowing a Null Value to a Data Source	1008
21.36	Contributing a UTCCodedTime Attribute in Active Directory	1010
21.37	Importing and Decoding the accountExpires Attribute	1011
21.38	Exporting and Encoding the accountExpires Attribute	1013

<b>Index</b>	<b>1017</b>
--------------	-------------

---

# Preface

In 1998, when Robbie first became involved with the Microsoft Windows 2000 Joint Development Program (JDP), there was very little data available on Active Directory (AD). In the following months and even after the initial release of Windows 2000, there were very few books or white papers to help early adopters of Active Directory get started. And some of the information that had been published was often inaccurate or misleading. Many early adopters had to learn by trial and error. As time passed, more and more informative books were published, which helped fill the information gap.

By the end of the second year of its release, there was an explosion of information on Active Directory. Not only were there more than 50 books published, but Microsoft also cleaned up their documentation on MSDN (<http://msdn.microsoft.com>) and their AD website (<http://www.microsoft.com/ad>). Now those sites have numerous white papers, many of which could serve as mini booklets. Other websites have popped up as well that contain a great deal of information on Active Directory. With Windows Server 2003 and Windows Server 2008, Microsoft has taken their level of documentation a step higher. Extensive information on Active Directory is available directly from any Windows Server 2003 or 2008 computer in the form of the Help and Support Center (available from the Start Menu). So with all this data available on Active Directory in the form of published books, white papers, websites, and even from within the operating system, why would you want to purchase this one?

In the summer of 2002, Robbie was thumbing through Tom Christiansen and Nathan Torkington's *Perl Cookbook* from O'Reilly, looking for help with an automation script that he was writing for Active Directory. It just so happened that there was a recipe that addressed the specific task he was trying to perform. In Cookbook parlance, a recipe provides instructions on how to solve a particular problem. We thought that since Active Directory is such a task-oriented environment, the Cookbook approach might be a very good format. After a little research, Robbie found there were books (often multiple) on nearly every facet of Active Directory, including introductory books, design guides, books that focused on migration, programming books, and reference books. The one type of book that he didn't see was a task-oriented "how to" book, which is exactly what the Cookbook format provides. With this was born the first

---

edition of *Active Directory Cookbook*, covering Active Directory tasks in Windows 2000 and Windows Server 2003 Active Directory.

In 2005, Laura E. Hunter revised the already popular *Active Directory Cookbook* to include an updated range of automation options, including the use of command-line tools and scripts that had been created by active members of the Directory Services community in the years since AD was first introduced.

Based on our experience, hours of research, and nearly a decade of hanging out on Active Directory newsgroups and mailing lists, we've compiled more than 500 recipes that should answer the majority of "How do I do X?" questions one could pose about Active Directory. And just as in the Perl community, where the *Perl Cookbook* was a great addition that sells well even today, we believe *Active Directory Cookbook*, Third Edition, will also be a great addition to any Active Directory library.

## Who Should Read This Book?

As with many of the books in the Cookbook series, *Active Directory Cookbook*, Third Edition, can be useful to anyone who wants to deploy, administer, or automate Active Directory. This book can serve as a great reference for those who have to work with Active Directory on a day-to-day basis. For those without much programming background, the command-line, VBScript, and PowerShell solutions are straightforward and provide an easy way to automate repetitive administrative tasks for any administrator.

The companion to this book, *Active Directory*, Fourth Edition, by Brian Desmond et al. (O'Reilly), is a great choice for those wanting a thorough description of the core concepts behind Active Directory, how to design an Active Directory infrastructure, and how to automate that infrastructure using Active Directory Service Interfaces (ADSI) and Windows Management Instrumentation (WMI). *Active Directory*, Fourth Edition, does not necessarily detail the steps needed to accomplish every possible task within Active Directory; that is more the intended purpose of this book. These two books, along with the supplemental information referenced within each, should be sufficient to answer most questions you have about Active Directory.

## What's in This Book?

This book consists of 21 chapters. Here is a brief overview of each chapter:

### Chapter 1, *Getting Started*

Sets the stage for the book by covering where you can find the tools used in the book, VBScript and PowerShell issues to consider, and where to find additional information.

---

Chapter 2, *Forests, Domains, and Trusts*

Covers how to create and remove forests and domains, update the domain mode or functional levels, create different types of trusts, and other administrative trust tasks.

Chapter 3, *Domain Controllers, Global Catalogs, and FSMOs*

Covers promoting and demoting domain controllers, finding domain controllers, enabling the global catalog, and finding and managing Flexible Single Master Operations (FSMO) roles. This will include coverage of the new Read-Only Domain Controller (RODC) that was introduced with Windows Server 2008.

Chapter 4, *Searching and Manipulating Objects*

Covers the basics of searching Active Directory: creating, modifying, and deleting objects, using LDAP controls, and importing and exporting data using LDAP Data Interchange Format (LDIF) and comma-separated variable (CSV) files.

Chapter 5, *Organizational Units*

Covers creating, moving, and deleting Organizational Units, and managing the objects contained within them.

Chapter 6, *Users*

Covers all aspects of managing user objects, including creating, renaming, moving, resetting passwords, unlocking, modifying the profile attributes, and locating users that have certain criteria (e.g., password is about to expire). This chapter includes coverage of the new Fine-Grained Password Policy feature that was introduced in Windows Server 2008.

Chapter 7, *Groups*

Covers how to create groups, modify group scope and type, and manage membership.

Chapter 8, *Computer Objects*

Covers creating computers, joining computers to a domain, resetting computers, and locating computers that match certain criteria (e.g., have been inactive for a number of weeks).

Chapter 9, *Group Policy Objects*

Covers how to create, modify, link, copy, import, back up, restore, and delete GPOs using the Group Policy Management Console and scripting interface, including new Group Policy features that were introduced in Windows Server 2008.

Chapter 10, *Schema*

Covers basic schema administration tasks, such as generating object identifiers (OIDs) and schemaIDGUIDs, how to use LDIF to extend the schema, and how to locate attributes or classes that match certain criteria (e.g., all attributes that are indexed).

Chapter 11, *Site Topology*

Covers how to manage sites, subnets, site links, and connection objects.

---

Chapter 12, *Replication*

Covers how to trigger and disable the Knowledge Consistency Checker (KCC), how to query metadata, force replication, and determine what changes have yet to replicate between domain controllers.

Chapter 13, *DNS and DHCP*

Covers creating zones and resource records, modifying DNS server configuration, querying DNS, and customizing the resource records a domain controller dynamically registers.

Chapter 14, *Security and Authentication*

Covers how to delegate control, view and modify permissions, view effective permissions, and manage Kerberos tickets.

Chapter 15, *Logging, Monitoring, and Quotas*

Covers how to enable auditing, diagnostics, DNS, NetLogon, and Kerberos and GPO logging; obtain LDAP query statistics; and manage quotas.

Chapter 16, *Backup, Recovery, DIT Maintenance, and Deleted Objects*

Covers how to back up Active Directory, perform authoritative and nonauthoritative restores, check DIT file integrity, perform online and offline defrags, and search for deleted objects.

Chapter 17, *Application Partitions*

Covers creating and managing application partitions.

Chapter 18, *Active Directory Application Mode and Active Directory Lightweight Directory Service*

Covers the new Active Directory Application Mode (ADAM) functionality that's available with R2.

Chapter 19, *Active Directory Federation Services*

Covers the new Active Directory Federation Services (AD FS) that are included with Windows Server 2003 R2.

Chapter 20, *Microsoft Exchange Server 2007 and Exchange Server 2003*

Covers common administrative tasks for Exchange Server 2003.

Chapter 21, *Microsoft Identity Lifecycle Manager*

Provides an introduction to Microsoft's Identity Integration Server (MIIS), a service that can be used to synchronize multiple directories or enforce data integrity within a single or multiple stores.

---

## Conventions Used in This Book

The following typographical conventions are used in this book:

### Constant width

Indicates classes, attributes, cmdlets, methods, objects, command-line elements, computer output, and code examples.

### Constant width *italic*

Indicates placeholders (for which you substitute an actual name) in examples and in registry keys.

### Constant width **bold**

Indicates user input.

### *Italic*

Introduces new terms and example URLs, commands, file extensions, filenames, directory or folder names, and UNC pathnames.



Indicates a tip, suggestion, or general note. For example, we'll tell you if you need to use a particular version or if an operation requires certain privileges.



Indicates a warning or caution. For example, we'll tell you if Active Directory does not behave as you'd expect or if a particular operation has a negative impact on performance.

## Using Code Examples

This book is here to help you get your job done. In general, you may use the code in this book in your programs and documentation. You do not need to contact us for permission unless you're reproducing a significant portion of the code. For example, writing a program that uses several chunks of code from this book does not require permission. Selling or distributing a CD-ROM of examples from O'Reilly books *does* require permission. Answering a question by citing this book and quoting example code does not require permission. Incorporating a significant amount of example code from this book into your product's documentation *does* require permission.

We appreciate, but do not require, attribution. An attribution usually includes the title, author, publisher, and ISBN. For example: *Active Directory Cookbook*, Third Edition, by Laura E. Hunter and Robbie Allen. Copyright 2009 O'Reilly Media, Inc., 978-0-596-52110-3.

If you feel your use of code examples falls outside fair use or the permission given above, feel free to contact us at [permissions@oreilly.com](mailto:permissions@oreilly.com).

---

## Safari® Books Online



When you see a Safari® Books Online icon on the cover of your favorite technology book, that means the book is available online through the O'Reilly Network Safari Bookshelf.

Safari offers a solution that's better than e-books. It's a virtual library that lets you easily search thousands of top tech books, cut and paste code samples, download chapters, and find quick answers when you need the most accurate, current information. Try it for free at <http://safari.oreilly.com>.

## We'd Like Your Feedback!

We at O'Reilly have tested and verified the information in this book to the best of our ability, but mistakes and oversights do occur. Please let us know about errors you may find, as well as your suggestions for future editions, by writing to:

O'Reilly Media, Inc.  
1005 Gravenstein Highway North  
Sebastopol, CA 95472  
800-998-9938 (in the U.S. or Canada)  
707-829-0515 (international or local)  
707-829-0104 (fax)

We have a web page for the book where we list errata, examples, or any additional information. You can access this page at:

<http://www.oreilly.com/catalog/9780596521103>

To comment or ask technical questions about this book, send email to:

[bookquestions@oreilly.com](mailto:bookquestions@oreilly.com)

For more information about our books, conferences, software, Resource Centers, and the O'Reilly Network, see our website at:

<http://www.oreilly.com>

## Acknowledgments

### Robbie Allen, from the First Edition

The people at O'Reilly were a joy to work with. I would like to thank Robert Denn for helping me get this book off the ground. I am especially grateful for Andy Oram's insightful and thought-provoking feedback.



- [The Toltec Art of Life and Death: A Story of Discovery here](#)
- [read online Intellectuals and Society \(2nd Edition\)](#)
- [download Dearly Devoted Dexter \(Dexter, Book 2\) pdf, azw \(kindle\)](#)
- [ECG Facts Made Incredibly Quick! \(2nd Edition\) pdf](#)
- [\*\*read Equality and Tradition: Questions of Value in Moral and Political Theory for free\*\*](#)
- [download online The Dutiful Rake](#)
  
- <http://conexdx.com/library/4-09-43--Boston-2013-Through-the-Eyes-of-the-Runners.pdf>
- <http://flog.co.id/library/Intellectuals-and-Society--2nd-Edition-.pdf>
- <http://betsy.wesleychapelcomputerrepair.com/library/Dearly-Devoted-Dexter--Dexter--Book-2-.pdf>
- <http://rodrigocaporal.com/library/The-Tragedy-of-Arthur--A-Novel.pdf>
- <http://musor.ruspb.info/?library/Equality-and-Tradition--Questions-of-Value-in-Moral-and-Political-Theory.pdf>
- <http://damianfoster.com/books/De-la-mis--re-symbolique.pdf>