Solutions for Administrators & Developers

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

Active Directory Cookbook™

Laura E. Hunter
& Robbie Allen

O'REILLY®

Windows Administration

O'REILLY®

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.

"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.

www.oreilly.com

US $59.99 CAN $59.99

ISBN: 978-0-596-52110-3

THIRD EDITION

Active Directory Cookbook™

Laura E. Hunter and Robbie Allen

O'REILLY®
Beijing • Cambridge • Farnham • Köln • Sebastopol • Taipei • Tokyo

Active Directory Cookbook™, Third Edition
by Laura E. Hunter and Robbie Allen

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*.

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.

ISBN: 978-0-596-52110-3

[M]

1229006171

Table of Contents

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*.

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

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.