Microsoft

Windows Server® 2008 Active Directory®

资源大全

Stan Reimer,
Conan Kezema,
Mike Mulcare, and
Byron Wright, with the
Microsoft Active Directory Team

China Edition
Published by Shanghai World Publishing Corporation

Resource Kit

世界图书出版公司

Microsoft

Windows® Server® 2008 Active Directory® Resource Kit

Stan Reimer, Conan Kezema, Mike Mulcare, and Byron Wright
with the Microsoft Active Directory Team

图书在版编目(CIP)数据

Windows Server 2008 Active Directory 资源大全:英文/(美)雷莫等著. -上海:上海世界图书出版公司,2008.10

ISBN 978 -7 -5062 -9296 -2

Ⅰ. W… Ⅱ. 雷… Ⅲ. 窗口软件-网络服务器-英文 Ⅳ. TP316.86

中国版本图书馆 CIP 数据核字(2008)第 164107 号

Windows Server 2008 Active Directory 资源大全

[美]斯坦·雷莫 科南·凯泽马 麦克·穆凯尔 拜伦·莱特 Microsoft Active Directory 团队 著

上海世界图书出版公司 出版发行
上海市尚文路 185 号 B 楼
邮政编码 200010
(公司电话:021 -63783016 转发行部)
上海竟成印务有限公司印刷
如发现印装质量问题,请与印刷厂联系
(质检科电话:021 -56422678)
各地新华书店经销

开本:787 ×960 1/16 印张:54 字数:1750 000
2008 年 10 月第 1 版 2008 年 10 月第 1 次印刷
ISBN 978 -7 -5062 -9296 -2/T·183
图字:09 -2008 -627 号
定价:238.00 元
http://www.wpcsh.com.cn
http://www.mspress.com.cn

To the three wonderful women in my life–Rhonda, Angela, and Amanda.
Your love and encouragement keep me going.

– Stan Reimer

I dedicate this book to the love of my life, Rhonda, and our precious sons, Brennan and Liam. Thank you for your continuous support and for being the reason that I do what I do. I also dedicate this book to the rest of my family, who are still trying to figure out what I actually do for a living.

– Conan Kezema

To my family–Nancy, James, Sean, and Patrick. Thanks always for your encouragement and support.

– Mike Mulcare

Tracey, Samantha, and Michelle, you are the reason I keep it going. Darrin, thanks for holding down the fort.

– Byron Wright

Acknowledgments

by Stan Reimer (for the team):

First of all, I want thank my coauthors for their hard work on this book. When I was first asked to lead this writing project, I looked around for the right people to work with me on this book and I couldn't have picked a better team.

Secondly, I want to thank the folks at Microsoft Press. This team includes Martin DelRe, the program manager, who kept poking us until we agreed to do this project, Karen Szall, the content development manager, and Maureen Zimmerman, the content project manager. I am sure that the problems we had keeping to the schedule on this book caused a few headaches for this group, but they were amazingly supportive and encouraging all the way through. Maureen had an amazing knack for reminding us when materials were due without making it feel like nagging.

Thanks to Bob Dean, the technical reviewer, for his valuable comments. Production for this book was professionally handled by Custom Editorial Productions Inc., with Linda Allen as the project manager, Cecilia Munzenmaier as the copy editor, and many others who toiled away in the background. As writers, we get to have all of the fun at the beginning of the process; these folks are still working on this long after we are done.

A Resource Kit doesn't come together without a lot of interaction with the product groups at Microsoft, as well as other technical experts, such as Directory Services MVPs. All of the chapters in this book have been reviewed by these experts and many of these experts contributed to the Direct from the Source, Direct from the Field, or How It Works sidebars that you will enjoy reading in this book. These reviewers and contributors include:

James McColl, Mike Stephens, Moon Majumdar, Judith Herman, Mark Gray, Linda Moore, Greg Robb, Barry Hartman, Christiane Soumahoro, Gautam Anand, Michael Hunter, Alain Lissoir, Yong Liang, David Hastie, Teoman Smith, Brian Lich, Matthew Rimer, David Fisher, Bob Drake, Rob Greene, Andrej Budja, Rob Lane, Gregoire Guetat, Donovan Follette, Pavan Kompelli, Sanjeev Balarajan, Fatih Colgar, Brian Desmond, Jose Luis Auricchio, Darol Timberlake, Peter Li, Elbio Abib, Ashish Sharma, Nick Pierson, Lu Zhao, and Antonio Calomeni.

by Conan Kezema:

Special thanks to my fellow coauthors for their hard work on this book. I would also like to thank Stan for the many opportunities he has provided over the years; he is a great friend and mentor.

Introduction

Welcome to the *Windows Server 2008 Active Directory Resource Kit*, your complete source for the information you need to design and implement Active Directory in Windows Server 2008.

The *Windows Server 2008 Active Directory Resource Kit* is a comprehensive technical resource for planning, deploying, maintaining, and troubleshooting an Active Directory infrastructure in Windows Server 2008. While the target audience for this Resource Kit is experienced IT professionals who work in medium-sized and large-sized organizations, anyone who wants to learn how to implement and manage Active Directory in Windows Server 2008 will find this Resource Kit invaluable.

One of the new features in Windows Server 2008 Active Directory is that the term *Active Directory* now covers a lot more territory than it did in previous iterations of this directory service. What was previously called Active Directory in Windows 2000 and Windows Server 2003 is now called Active Directory Domain Services (AD DS), and several more directory service components have been included under the Active Directory umbrella. These include Active Directory Lightweight Directory Services (AD LDS), Active Directory Certificate Services (AD CS), Active Directory Rights Management Services (AD RMS), and Active Directory Federation Services (AD FS).

Within this Resource Kit you'll find in-depth technical information on how Active Directory works in Windows Server 2008. In addition, you will find detailed task-based guidance for implementing and maintaining the Active Directory infrastructure. You'll also find numerous sidebars–contributed by members of the Active Directory product team, other directory experts at Microsoft, and directory services MVPs–that provide deep insight into how Active Directory works, best practices for designing and implementing Active Directory, and invaluable troubleshooting tips. Finally, the companion CD includes deployment tools, templates, and many sample scripts that you can use and customize to help you automate various aspects of managing Active Directory in enterprise environments.

Overview of Book

This book is divided into the following five parts with the following chapters:

Part I – Windows Server 2008 Active Directory Overview

- **Chapter 1 – "What's New in Active Directory for Windows Server 2008"** This chapter provides an overview of the new features that are available in Windows Server 2008. If you know Windows Server 2003 Active Directory, this is a good place for you to get a quick overview of some of the new material that will be covered in this book.

- **Chapter 2 – "Active Directory Domain Services Components"** This chapter provides an overview of Active Directory Domain Services–if you are somewhat new to Active Directory, this is a great chapter to get you started on the terms and concepts that make up AD DS.
- **Chapter 3 – "Active Directory Domain Services and Domain Name System"** One of the most critical components that you need in order to make AD DS work efficiently is a properly implemented DNS infrastructure. This chapter provides information on how to do this.
- **Chapter 4 – "Active Directory Domain Services Replication"** In order to work with AD DS, you will need to understand replication. This chapter provides all of the details of how AD DS replication works and how to configure it.

Part II – Designing and Implementing Windows Server 2008 Active Directory

- **Chapter 5 – "Designing the Active Directory Domain Services Structure"** Before deploying AD DS, you need to create a design that meets your organization's requirements. This chapter provides the in-depth information that you will need to do that planning.
- **Chapter 6 – "Installing Active Directory Domain Services"** Installing AD DS on a Windows Server 2008 computer is pretty easy, but there several variations on how to perform the installation. This chapter describes all of the options and the reasons for choosing each one.
- **Chapter 7 – "Migrating to Active Directory Domain Services"** Many organizations are already running a previous version of Active Directory. This chapter provides the details on how to deploy Windows Server 2008 domain controllers in this environment, and how to migrate the Active Directory environment to Windows Server 2008.

Part III – Administering Windows Server 2008 Active Directory

- **Chapter 8 – "Active Directory Domain Services Security"** AD DS provides the core network authentication and authorization services in many organizations. This chapter describes how AD DS security works and the steps you can take to secure your AD DS environment.
- **Chapter 9 – "Delegating the Administration of Active Directory Domain Services"** One of the options in implementing AD DS is that you can delegate many administrative tasks to other administrators without granting them domain level permissions. This chapter describes how AD DS permissions work and how to delegate them.
- **Chapter 10 – "Managing Active Directory Objects"** Most of your time as an AD DS administrator will be spent managing AD DS objects like users, groups and organizational units. This chapter deals with how to manage these objects individually, but also provides details on how to manage large numbers of these objects by using scripts.

- **Chapter 11 – "Introduction to Group Policy"** A central component in a Windows Server 2008 network management system is Group Policy. With Group Policy, you can manage many desktop settings as well as configure security. This chapter begins by explaining what Group Policy objects are and shows how to apply and filter Group Policy objects.
- **Chapter 12 – "Using Group Policy to Manage User Desktops"** One of the important tasks you can perform with Group Policy is configuring user desktops. In Windows Server 2008 and Windows Vista, there are several thousand Group Policy settings available. This chapter describes not only how to apply the policies, but also which policies are most important to apply.
- **Chapter 13 – "Using Group Policy to Manage Security"** Another important task that you can perform with Group Policy is applying security settings. This includes settings that will be applied to all users and computers in the domain as well as settings that can be applied to individual computers or users. This chapter provides the details on how to configure security by using Group Policy.

Part IV – Maintaining Windows Server 2008 Active Directory

- **Chapter 14 – "Monitoring and Maintaining Active Directory"** This chapter prepares you to maintain your Active Directory infrastructure after you deploy it. This chapter covers how to monitor your AD DS environment, and how to maintain the AD DS domain controllers.
- **Chapter 15 – "Active Directory Disaster Recovery"** Because of the central role that AD DS has in many corporations, it is critical that you know how to prepare for and recover from disasters within your AD DS environment. This chapter details how you can do this.

Part V – Identity and Access Management with Active Directory

- **Chapter 16 – "Active Directory Lightweight Directory Services"** AD LDS is one of the new server roles that is included under the Active Directory umbrella in Windows Server 2008. AD LDS is designed to be an application directory–this chapter describes how you can deploy and manage your AD LDS environment.
- **Chapter 17 – "Active Directory Certificate Services"** AD CS can be used to provide the public key infrastructure that provides digital certificates that are so critical for many network security implementations. This chapter describes how to plan and implement AD CS.
- **Chapter 18 – "Active Directory Rights Management Services"** AD RMS provides the tools to apply persistent usage policies to information that stays with the information even as it is moved around or outside the organization. This chapter details how to implement AD RMS.

- **Chapter 19 – "Active Directory Federation Services"** AD FS provides a means to enable users to access multiple Web-based applications in their organization or in other organizations while only authenticating once. This chapter describes the AD FS deployment scenarios and how to implement them.

Document Conventions

The following conventions are used in this book to highlight special features and usage:

Reader Aids

The following reader aids are used throughout this book to point out useful details:

Reader Aid	Meaning
Note	Underscores the importance of a specific concept or highlights a special case that might not apply to every situation
Important	Calls attention to essential information that should not be disregarded
Caution	Warns you that failure to take or avoid a specified action can cause serious problems for users, systems, data integrity, and so on
On the CD	Calls attention to a related script, tool, template, or job aid on the companion CD that helps you perform a task described in the text
More Info	Points out Web sites or other related material that you can access to get more details about a topic described in the text
Security Alert	Emphasizes information or tasks that are essential for maintaining a secure environment or identifies events that indicate a potential security incident

Sidebars

The following sidebars are used throughout this book to provide added insight, tips, and advice concerning Windows Server 2008 Active Directory:

Sidebar	Meaning
Direct from the Source	Contributed by experts at Microsoft to provide "from-the-source" insight into how Active Directory in Windows Server 2008 works, best practices for planning and implementing the Active Directory server roles, and troubleshooting tips
Direct from the Field	Contributed by directory service MVPs to provide real-world insight into best practices for planning and implementing the Active Directory server roles and troubleshooting tips
How It Works	Provides unique glimpses of Windows Server 2008 Active Directory features and how they work

Command-Line Examples

The following style conventions are used in documenting command-line examples throughout this book:

Style	Meaning
Bold font	Used to indicate user input (characters that you type exactly as shown)
Italic font	Used to indicate variables for which you need to supply a specific value (for example, *filename* can refer to any valid file name)
`Monospace font`	Used for code samples and command-line output
%SystemRoot%	Used for environment variables

Companion CD

The companion CD is a valuable addition to this book. Many of the tools and resources mentioned in the chapters are on the CD itself; you can access other tools and resources via links from the CD.

For documentation of the contents and structure of the companion CD, see the Readme.txt file on the CD.

Management Scripts

A set of scripts to manage Active Directory is included on the CD. Among them are scripts to get information about Active Directory objects and scripts to create or modify these objects. These scripts all require Windows PowerShell. The following scripts are included on the CD:

- **AddUserToGroup.ps1** Adds a user account to a group in the same OU
- **CreateAndEnableUserFromCSV.ps1** Creates an enabled user account by reading a .csv file
- **CreateGroup.ps1** Creates a group in Active Directory in the OU and domain specified
- **CreateObjectInAD.ps1** Creates an object in Active Directory
- **CreateOU.ps1** Creates an organizational unit in Active Directory
- **CreateUser.ps1** Creates a user account in Active Directory
- **EnableDisableUserSetPassword.ps1** Enables or disables a user account and sets the password
- **GetDomainPwdSettings.ps1** Obtains the password policy settings for a domain
- **GetModifiedDateFromAD.ps1** Lists the last modified date of a specific user onto a local or remote domain

- **ListUserLastLogon.ps1** Lists the last logon date of a specific user onto a local or remote domain
- **LocateDisabledUsers.ps1** Locates disabled user accounts in a local or remote domain
- **LocateLockedOutUsers.ps1** Locates locked out user accounts a local or remote domain
- **LocateOldComputersNotLogon.ps1** Locates computer accounts in a local or remote domain that have not logged on for a specified number of days
- **LocateOldUsersNotLogOn.ps1** Scans a local or remote domain for user accounts that have not logged onto the domain for an extended period of time that is specified in days
- **ModifyUser.ps1** Modifies user attributes in Active Directory
- **QueryAD.ps1** Queries Active Directory for objects such as users, groups, computers, and so on
- **UnlockLockedOutUsers.ps1** Unlocks user accounts that are locked out

In addition to these scripts, many of the chapters contain references to additional scripts that perform the management tasks included in that chapter.

Full documentation of the contents and structure of the companion CD can be found in the Readme.txt file on the CD.

Using the Scripts

The companion CD includes scripts that are written in VBScript (with a .vbs file extension) and Windows PowerShell (with a .ps1 file extension).

The VBScript scripts on the companion CD are identified with the .vbs extension. To use those scripts, double-click them or execute them directly from a command prompt.

The Windows PowerShell scripts require that you have Windows PowerShell installed and that you have configured Windows PowerShell to run unsigned scripts. You can run the Windows PowerShell scripts on Windows XP SP2, Windows Server 2003 SP1, Windows Vista, or Windows Server 2008. In order for the scripts to work, all computers must be members of a Windows Server 2008 domain.

> **Note** For information about the system requirements for running the scripts on the CD, see the System Requirements page at the end of the book.

Find Additional Content Online

As new or updated material becomes available that complements your book, it will be posted online 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.

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=109208 to get your downloadable content. This content is always up-to-date and available to all readers.

Resource Kit Support Policy

Every effort has been made to ensure the accuracy of this book and the companion CD content. Microsoft Press provides corrections to this book through the Web at the following location:

http://www.microsoft.com/learning/support/search.asp.

If you have comments, questions, or ideas regarding the book or companion CD content, or if you have questions that are not answered by querying the Knowledge Base, please send them to Microsoft Press by using either of the following methods:

E-mail:

rkinput@microsoft.com

Postal Mail:

Microsoft Press

Attn: Windows Server 2008 Active Directory Resource Kit

One Microsoft Way

Redmond, WA 98052-6399

Please note that product support is not offered through the preceding mail addresses.
For product support information, please visit the Microsoft Product Support Web site at the following address:

http://support.microsoft.com

Contents at a Glance

Table of Contents

Part II Designing and Implementing Windows Server 2008 Active Directory