

Introducing Windows Server 2008

*Mitch Tulloch with the
Microsoft Windows Server
Team*

[Purchase select Microsoft Press books at a discount](#)
(available in the United States only)

To learn more about this book, visit Microsoft Learning at
<http://www.microsoft.com/MSPress/books/11163.aspx>

9780735624214
Publication Date: May 2007

Microsoft®
Press

Additional Resources for IT Professionals

Published and Forthcoming Titles from Microsoft Press

→ Windows Server

Microsoft® Windows Server® 2003
Resource Kit

Microsoft MVPs and Partners with
Microsoft Windows Server Team
978-0-7356-2232-6

Microsoft Windows Server 2003
Administrator's Companion
Second Edition

Charlie Russel, Sharon Crawford,
and Jason Gerend
978-0-7356-2047-6

Microsoft Windows Server 2003
Inside Out

William R. Stanek
978-0-7356-2048-3

Microsoft Windows Server 2003
Administrator's Pocket Consultant
Second Edition

William R. Stanek
978-0-7356-2245-6

→ Windows Client

Windows Vista™
Resource Kit

Tulloch, Northrup, Honeycutt,
Russel, and Wilson with the
Microsoft Windows Vista Team
978-0-7356-2283-8

Windows Vista
Administrator's Pocket Consultant

William R. Stanek
978-0-7356-2296-8

Microsoft Windows® XP
Professional
Resource Kit
Third Edition

The Microsoft Windows Team with
Charlie Russel and Sharon Crawford
978-0-7356-2167-1

Microsoft Windows XP
Professional
Administrator's Pocket Consultant
Second Edition

William R. Stanek
978-0-7356-2140-4

Microsoft Windows Command-Line
Administrator's Pocket Consultant

William R. Stanek
978-0-7356-2038-4

→ SQL Server 2005

Microsoft SQL Server™ 2005
Administrator's Pocket Consultant

William R. Stanek
978-0-7356-2107-7

Microsoft SQL Server 2005
Administrator's Companion

Whalen, Garcia, et al.
978-0-7356-2198-5

Inside Microsoft SQL Server 2005:
The Storage Engine

Kalen Delaney
978-0-7356-2105-3

Inside Microsoft SQL Server 2005:
T-SQL Programming

Itzik Ben-Gan, Dejan Sarka, and
Roger Wolter
978-0-7356-2197-8

→ Exchange Server 2007

Microsoft Exchange Server 2007
Administrator's Companion

Walter Glenn and Scott Lowe
978-0-7356-2350-7

Microsoft Exchange Server 2007
Administrator's Pocket Consultant

William R. Stanek
978-0-7356-2348-4

→ Scripting

Microsoft Windows PowerShell™
Step by Step

Ed Wilson
978-0-7356-2395-8

Microsoft VBScript
Step by Step

Ed Wilson
978-0-7356-2297-5

Microsoft Windows
Scripting with WMI:
Self-Paced Learning Guide

Ed Wilson
978-0-7356-2231-9

Advanced VBScript for Microsoft
Windows Administrators

Don Jones and Jeffery Hicks
978-0-7356-2244-9

RELATED TITLES



Microsoft Office
SharePoint® Server
2007 *Administrator's Companion*
Bill English with the
Microsoft SharePoint
Community Experts
978-0-7356-2282-1



Microsoft Windows
Security
Resource Kit
Second Edition
Ben Smith and Brian
Komar with the
Microsoft Security
Team
978-0-7356-2174-9



Microsoft Windows
Small Business
Server 2003 R2
Administrator's Companion
Charlie Russel and
Sharon Crawford
978-0-7356-2280-7



Microsoft Internet
Security and
Acceleration (ISA)
Server 2004
Administrator's Pocket Consultant
Bud Ratliff and Jason
Ballard with the Microsoft
ISA Server Team
978-0-7356-2188-6

Resources for IT Professionals



Administrator's Pocket Consultant

- Practical, portable guide for fast answers when you need them
- Focus on core operations and support tasks
- Organized for quick, precise reference—to get the job done



Administrator's Companion

- Comprehensive, one-volume guide to deployment and system administration
- Real-world insights, procedures, troubleshooting tactics, and workarounds
- Fully searchable eBook on CD



Resource Kit

- In-depth technical information and tools from those who know the technology best
- Definitive reference for deployment and operations
- Essential toolkit of resources, including eBook, on CD



Self-Paced Training Kit

- Two products in one: official exam prep guide + practice tests
- Features lessons, exercises, and case scenarios
- Comprehensive self-tests; trial software; eBook on CD

Available in 2008 from Microsoft Press

Windows Server

Windows Server® 2008
Resource Kit
978-0-7356-2361-3

Windows Server 2008
Active Directory®
Resource Kit
978-0-7356-2515-0

Windows Server 2008
Virtualization
Resource Kit
978-0-7356-2517-4

Windows Server 2008
Security *Resource Kit*
978-0-7356-2504-4

Windows® Administration
*Resource Kit: Productivity
Solutions For IT Professionals*
978-0-7356-2431-3

Windows Server 2008
Networking Guide
978-0-7356-2422-1

Windows Server 2008 TCP/IP
Protocols and Services
978-0-7356-2447-4

Windows Server 2008
Inside Out
978-0-7356-2438-2

Windows Server 2008
Terminal Services
978-0-7356-2516-7

Windows Server 2008
Administrator's Companion
978-0-7356-2505-1

Windows Server 2008
Administrator's Pocket Consultant
978-0-7356-2437-5

Windows Group Policy Guide,
Second Edition
978-0-7356-2514-3

Understanding IPv6,
Second Edition
978-0-7356-2446-7

Internet Information Services

Internet Information
Services (IIS) 7.0
Administrator's Pocket Consultant
978-0-7356-2364-4

Internet Information
Services (IIS) 7.0
Resource Kit
978-0-7356-2441-2

Scripting

Windows PowerShell™
Scripting Guide
978-0-7356-2279-1

Windows PowerShell
& Command-line
Administrator's Pocket Consultant
978-0-7356-2262-3

Certification

MCITP Self-Paced Training Kit
(Exams 70-640, 70-642,
70-643, 70-646): Windows Server
Administrator Core Requirements
978-0-7356-2508-2

MCITP Self-Paced Training Kit
(Exam 70-640): Configuring
Windows Server 2008
Active Directory
978-0-7356-2513-6

MCITP Self-Paced Training Kit
(Exam 70-642): Configuring
Windows Server 2008
Network Infrastructure
978-0-7356-2512-9

MCITP Self-Paced Training Kit
(Exam 70-643): Configuring
Windows Server 2008
Applications Platform
978-0-7356-2511-2

MCITP Self-Paced Training Kit
(Exam 70-646): Windows Server
2008 Administrator
978-0-7356-2510-5

MCITP Self-Paced Training Kit
(Exam 70-647): Windows Server
2008 Enterprise Administrator
978-0-7356-2509-9

See our full line of learning resources at: microsoft.com/mspress and microsoft.com/learning

Microsoft®

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

Copyright © 2007 by Microsoft Corporation

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: 2007924650

Printed and bound in the United States of America.

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

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

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

Chapter 4 contains the “From the Experts: WMI Remote Connection” sidebar. Copyright © 2007 by Alain Lissor.

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, Active Directory, ActiveX, Aero, BitLocker, ClearType, Direct3D, Excel, Internet Explorer, Microsoft Dynamics, MSDN, MS-DOS, Outlook, PowerPoint, SharePoint, SQL Server, Terminal Services RemoteApp, Visual Basic, Visual Studio, Visual Web Developer, Win32, Windows, Windows CardSpace, Windows Live, Windows Media, Windows Mobile, Windows NT, Windows PowerShell, Windows Server, Windows Server System, Windows Vista, and WinFX 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: Martin DelRe

Developmental Editor: Karen Szall

Project Editor: Denise Bankaitis

Body Part No. X13-72717

Table of Contents

<i>Preface</i>	xiii
1 Introduction	1
What's Between the Sheets	3
Acknowledgments	4
One Last Thing—Humor	7
2 Usage Scenarios	9
Providing an Identity and Access Infrastructure	10
Ensuring Security and Policy Enforcement	10
Easing Deployment Headaches	11
Making Servers Easier to Manage	12
Supporting the Branch Office	13
Providing Centralized Application Access	13
Deploying Web Applications and Services	14
Ensuring High Availability	14
Ensuring Secure and Reliable Storage	15
Leveraging Virtualization	16
Conclusion	16
3 Windows Server Virtualization	17
Why Enterprises Love Virtualization	17
Server Consolidation	18
Business Continuity	18
Testing and Development	19
Application Compatibility	19
Virtualization in the Datacenter	19

 **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/

Virtualization Today	20
Monolithic Hypervisor	22
Microkernelized Hypervisor	22
Understanding Virtualization in Windows Server 2008	24
Partition 1: Parent	25
Partition 2: Child with Enlightened Guest	26
Partition 3: Child with Legacy Guest	27
Partition 4: Child with Guest Running Linux	28
Features of Windows Server Virtualization	28
Managing Virtual Machines in Windows Server 2008	29
System Center Virtual Machine Manager 2007	36
SoftGrid Application Virtualization	36
Conclusion	37
Additional Reading	37
4 Managing Windows Server 2008	39
Performing Initial Configuration Tasks	39
Using Server Manager	42
Managing Server Roles	44
ServerManagerCmd.exe	50
Remote Server Administration Tools	53
Other Management Tools	56
Group Policy	56
Windows Management Instrumentation	59
Windows PowerShell	64
Microsoft System Center	68
Conclusion	69
Additional Resources	69
5 Managing Server Roles	71
Understanding Roles, Role Services, and Features	71
Available Roles and Role Services	72
Available Features	83

Adding Roles and Features	95
Using Initial Configuration Tasks	97
Using Server Manager	104
From the Command Line	105
Conclusion	108
Additional Reading	108
6 Windows Server Core	109
What Is a Windows Server Core Installation?	109
Understanding Windows Server Core	111
The Rationale for Windows Server Core	115
Performing Initial Configuration of a Windows Server Core Server	118
Performing Initial Configuration from the Command Line	118
Managing a Windows Server Core Server	130
Local Management from the Command Line	130
Remote Management Using Terminal Services	137
Remote Management Using the Remote Server Administration Tools	140
Remote Administration Using Group Policy	141
Remote Management Using WinRM/WinRS	142
Windows Server Core Installation Tips and Tricks	143
Conclusion	147
Additional Resources	147
7 Active Directory Enhancements	149
Understanding Identity and Access in Windows Server 2008	149
Understanding Identity and Access	149
Identity and Access in Windows 2000 Server	150
Identity and Access in Windows Server 2003	151
Identity and Access in Windows Server 2003 R2	152
Identity and Access in Windows Server 2008	153
Active Directory Domain Services	158
AD DS Auditing Enhancements	158
Read-Only Domain Controllers	164
Restartable AD DS	168
Granular Password and Account Lockout Policies	169

Active Directory Lightweight Directory Services	172
Active Directory Certificate Services	176
Certificate Web Enrollment Improvements	176
Network Device Enrollment Service Support	177
Online Certificate Status Protocol Support	177
Enterprise PKI and CAPI2 Diagnostics	179
Other AD CS Enhancements	180
Active Directory Federation Services	182
Active Directory Rights Management Services	186
Conclusion	187
Additional Resources	187
8 Terminal Services Enhancements	189
Core Enhancements to Terminal Services	190
Remote Desktop Connection 6.0	191
Single Sign-On for Domain-joined Clients	200
Other Core Enhancements	201
Installing and Managing Terminal Services	209
Terminal Services RemoteApp	216
Using TS RemoteApp	217
Benefits of TS RemoteApp	225
Terminal Services Web Access	226
Using TS Web Access	227
Benefits of TS Web Access	232
Terminal Services Gateway	232
Implementing TS Gateway	235
Benefits of TS Gateway	237
Terminal Services Licensing	238
Other Terminal Services Enhancements	243
Terminal Services WMI Provider	243
Windows System Resource Manager	246
Terminal Services Session Broker	247
Conclusion	249
Additional Resources	250

9	Clustering Enhancements	251
	Failover Clustering Enhancements	252
	Goals of Clustering Improvements	253
	Understanding the New Quorum Model	254
	Understanding Storage Enhancements	256
	Understanding Networking and Security Enhancements	259
	Other Security Improvements	261
	Validating a Clustering Solution	261
	Tips for Validating Clustering Solutions	266
	Setting Up and Managing a Cluster	267
	Creating a Highly Available File Server	269
	Performing Other Cluster Management Tasks	273
	Network Load Balancing Enhancements	278
	Conclusion	283
	Additional Resources	283
10	Network Access Protection	285
	The Need for Network Access Protection	286
	Understanding Network Access Protection	287
	What NAP Does	288
	NAP Enforcement Methods	289
	Understanding the NAP Architecture	297
	A Walkthrough of How NAP Works	299
	Implementing NAP	301
	Choosing Enforcement Methods	302
	Phased Implementation	303
	Configuring the Network Policy Server	307
	Configuring NAP Clients	317
	Troubleshooting NAP	319
	Conclusion	339
	Additional Resources	340

11	Internet Information Services 7.0	341
	Understanding IIS 7.0 Enhancements	341
	Security and Patching	342
	Administration Tools	351
	Configuration and Deployment	360
	Diagnostics	365
	Extensibility	368
	What's New in IIS 7.0 in Windows Server 2008	370
	The Application Server Role	371
	Conclusion	374
	Additional Resources	375
12	Other Features and Enhancements	377
	Storage Improvements	378
	File Server Role	378
	Windows Server Backup	381
	Storage Explorer	384
	SMB 2.0	386
	Multipath I/O	387
	iSCSI Initiator	390
	iSCSI Remote Boot	397
	iSNS Server	401
	Networking Improvements	402
	Security Improvements	407
	Other Improvements	414
	Conclusion	419
	Additional Resources	419
13	Deploying Windows Server 2008	421
	Getting Windows Server 2008	421
	Installing Windows Server 2008	422
	Manual Installation	422
	Unattended Installation	423

Using Windows Deployment Services	423
Multicast Deployment	424
TFTP Windowing	427
EFI x64 Network Boot Support	430
Solution Accelerator for Windows Server Deployment.	431
Understanding Volume Activation 2.0	432
Conclusion	439
Additional Resources	440
14 Additional Resources	441
Product Home Page	441
Microsoft Windows Server TechCenter	442
Microsoft Download Center	442
Microsoft Connect.....	443
Microsoft TechNet.....	445
Beta Central	445
TechNet Events.....	446
TechNet Virtual Labs.....	448
TechNet Community Resources	448
TechNet Columns.....	451
TechNet Magazine.....	451
TechNet Flash Newsletter.....	451
MSDN	451
Blogs	452
Blogs by MVPs	453
Channel 9	454
Microsoft Press Books.....	454
Conclusion	455
Index	457



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/

Active Directory Enhancements

In this chapter:

Understanding Identity and Access in Windows Server 2008	149
Active Directory Domain Services	158
Active Directory Lightweight Directory Services	172
Active Directory Certificate Services	176
Active Directory Federation Services	182
Active Directory Rights Management Services	186
Conclusion	187
Additional Resources	187

Active Directory and its related services form the foundation for enterprise networks running Microsoft Windows, and the new features and enhancements to Active Directory and its related services in Windows Server 2008 are numerous. This chapter takes a look at these enhancements and at the direction in which Active Directory and its related services are heading as an integrated identity and access platform for enterprises—that is, as a platform for provisioning and managing network identity.

Understanding Identity and Access in Windows Server 2008

Before we jump in and examine the various enhancements to Active Directory and its related services in Windows Server 2008, however, let's first step back a bit and get the big picture of how Active Directory and its related services have been evolving since they were first introduced in Windows 2000 Server and what these services are becoming in Windows Server 2008 and beyond. It's important to understand this big picture, as otherwise the many improvements to Active Directory and related services in Windows Server 2008 might seem like a miscellaneous grab-bag of changes without much in common. But they have a lot in common as we'll shortly see.

Understanding Identity and Access

So why is identity and access (IDA) important to enterprises? Think for a moment about what goes on when a user on your network needs access to confidential business information stored on a server. Tony is in the Marketing department, and he needs access to a product

specification so that he can work on a marketing presentation for a customer. The document containing the specification is stored on a server on the company's network, and Tony tries to open the document so that he can cut and paste information contained in it into his presentation. To safeguard such specifications, you'd like your IDA infrastructure to do the following:

1. Determine who the user is who wants to use the document.
2. Grant the user the appropriate level of access to the document.
3. Protect confidential information contained in the document.
4. Maintain a record of interaction concerning the user's accessing of the document.

For example, you might want to restrict access to product specifications to full-time employees (FTEs) only and provide read-only access to users in the Marketing department so that they can view but not modify specifications. You might also want to prevent Marketing department users from copying and pasting text from specifications into other documents. And you might want an audit trail showing the day and time that the user accessed the specification.

The challenge of implementing an IDA solution that can do all of this becomes even greater once you start extending the boundaries of your enterprise with "anywhere access" devices, Web services, and collaboration tools like e-mail and instant messaging. It becomes even more complicated once you have to start applying the IDA process not just to FTEs but also to contractors, temps, customers, and external partners. The challenge is to build an IDA solution that can handle all these different scenarios, and Microsoft has steadily been working toward this goal since Active Directory was first released with Windows 2000 Server. Let's briefly summarize the evolution of Microsoft's IDA solution, beginning with Windows 2000 Server and working up to the current platform for Windows Server 2003 R2 and then to Windows Server 2008 and beyond.

Identity and Access in Windows 2000 Server

Active Directory directory service is a Windows-based directory service that was first introduced in Windows 2000 Server. Active Directory directory service stores information about various kinds of objects on a network—such as users, groups, computers, printers, and shared folders—and it makes this information available to users who need to access these resources and administrators who need to manage them. Active Directory provides network users with controlled access to permitted resources anywhere on the network using a single logon process. Active Directory directory service also provides administrators with an intuitive, hierarchical view of the network and its resources, and it provides a single point of administration for all network objects.

Windows 2000 Server also included a separate component, called Certificate Services, that can be used to set up a certificate authority (CA) for issuing digital certificates as part of a Public Key Infrastructure (PKI). These certificates can be used to provide authentication for users and computers on your network to secure e-mail, provide Web-based authentication,

and support smart-card authentication. Certificate Services also provides customizable services for issuing and managing certificates for your enterprise. What's important to understand here is that in Windows 2000 Server, Active Directory directory service and Certificate Services are two separate components that are not integrated together. In other words, the two services are managed separately and have policy implemented differently.

In addition to these two built-in IDA services, Microsoft also released an out-of-band service for Windows 2000 Server called Microsoft Metadirectory Services (MMS). In its final version, MMS 2.2 was an enterprise metadirectory that enterprises could use to integrate all their various directories together into a single consolidated central repository. MMS 2.2 consisted of one or more metadirectory servers, management agents, and the connected directories, and it provided users with access to this consolidated information via Lightweight Directory Access Protocol (LDAP). The goal of MMS 2.2 was to provide enterprises with a provisioning solution that could be used to effectively provide consistent identity management across many different databases and directories. For example, if you had both an Active Directory directory service infrastructure and a Lotus Notes infrastructure and you wanted Active Directory directory service users to be able to look up e-mail addresses from the Lotus Notes directory, MMS 2.2 could make this possible. MMS 2.2 could also simplify the deployment of Active Directory directory service for enterprises that already had information about employees or customers stored in other directories by enabling real-time synchronization of information from these directories into Active Directory directory service. Finally, MMS 2.2 could also be used to simplify the migration and consolidation of multiple directories into Active Directory directory service.

Identity and Access in Windows Server 2003

Although these Windows 2000 Server offerings did meet the needs of some enterprises, they were still provided as separate services and MMS was even a totally separate product. Customers wanted something more integrated, and they also wanted additional IDA features, such as document rights protection and role-based authorization. In addition to making improvements to how Active Directory directory service and Certificate Services work and how they are managed, Microsoft added a new feature called Authorization Manager to Windows 2003 Server that provided role-based authorization for users of line-of-business applications. Although Active Directory directory service by itself provides object-based access control using ACLs, the role-based access control (RBAC) provided by Authorization Manager enables permissions to be managed in terms of the different job roles users might have. Authorization Manager works by providing a set of COM-based runtime interfaces that enables an application to manage and verify a client's requests to perform operations using the application. Authorization Manager also includes an MMC snap-in that application administrators can use to manage different user roles and permissions.

Another IDA service that Microsoft released for Windows Server 2003 is Windows Rights Management Service (RMS), an information-protection technology that works with RMS-enabled applications to help businesses safeguard valuable digital information from

unauthorized use whether online or offline and whether inside the firewall or outside the firewall. Windows RMS was also designed to help organizations comply with a growing number of regulatory requirements that mandated information protection, including the U.S. Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), and others. To use Windows RMS, enterprises can create centralized custom usage policy templates, such as “Confidential – Read Only,” that can work with any RMS-enabled client and can be directly applied to sensitive business information such as financial reports, product specifications, or e-mail messages. Implementing Windows RMS requires an Active Directory directory service infrastructure, a PKI, and Internet Information Services—all of which are included in Windows Server 2003. In addition, RMS-enabled client applications such as Microsoft Office 2003 and Internet Explorer are needed, plus Microsoft SQL Server to provide the underlying database for the service.

While these additional IDA services and add-ons for Active Directory directory service were being released, Microsoft also released a follow-up to MMS 2.2 called Microsoft Identity Integration Server (MIIS) 2003, which provides a centralized service that stores and integrates identity information for organizations with multiple directories. It also provides a unified view of all known identity information about users, applications, and resources on a network. MIIS 2003 is designed for life-cycle management of identity and access to simplify the provisioning of new user accounts, strong credentials, access policies, rights management policies, and so on. MIIS 2003 is available in two versions. First, there’s Microsoft Identity Integration Server 2003 SP1, Enterprise Edition, which includes support for identity integration/directory synchronization, account provisioning/deprovisioning, and password synchronization and management. And second, there’s Identity Integration Feature Pack 1a for Microsoft Windows Server Active Directory, a free download that provides the same functionality as Microsoft Identity Integration Server 2003 SP1, Enterprise Edition (identity integration/directory synchronization, account provisioning/deprovisioning, and password synchronization) but only between Active Directory directory service, Active Directory Application Mode (ADAM), and Microsoft Exchange Server 2000 and later. Enterprises that need to interface with repositories other than Active Directory, ADAM, or Exchange Server, however, must use MIIS 2003, Enterprise Edition, rather than the free Feature Pack version.

Identity and Access in Windows Server 2003 R2

With the R2 release of Windows Server 2003, Microsoft added two more IDA services to the slate of various services already available on Windows Server 2003 either as in-box services, downloadable add-ons, or separate server products built upon Active Directory directory services. These two new IDA services are Active Directory Application Mode and Active Directory Federation Services.

Active Directory Application Mode (ADAM) is essentially a standalone version of Active Directory directory service that is designed specifically for use with directory-enabled

applications. ADAM does not require or depend upon Active Directory forests or domains, so you can use it in a workgroup scenario on standalone servers if desired—you don't have to install it on a domain controller. In addition, ADAM stores and replicates only application-related information and does not store or replicate information about network resources, such as users, groups, or computers. And because ADAM is not an operating system service, you can even run multiple instances of ADAM on a single computer, with each instance of ADAM supporting a different directory-enabled application and having its own directory store, assigned LDAP and SSL ports, and application event log. ADAM is provided as an optional component of Windows Server 2003 R2, but there's also a downloadable version that can be installed on either Windows Server 2003 or Windows XP.

Active Directory Federation Services (ADFS) is another optional component of Windows Server 2003 R2 that provides Web single sign-on (SSO) functionality to authenticate a user to multiple Web applications over the life of a single online session. ADFS works by securely sharing digital identity and entitlement rights across security and enterprise boundaries, and it supports the WS-Federation Passive Requestor Profile (WS-F PRP) Web Services protocol. ADFS is tightly integrated with Active Directory, and it can work with both Active Directory directory services and ADAM. Using ADFS, an enterprise can extend its existing Active Directory infrastructure to the Internet to provide access to resources that are offered by trusted partners across the Internet. These trusted partners can be either external third parties or additional departments or subsidiaries within the enterprise.

Identity and Access in Windows Server 2008

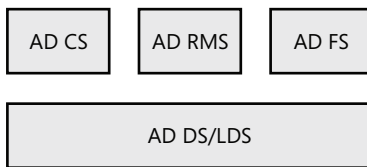
Looking back over this evolution of Active Directory-based IDA services since Windows 2000 Server, we have the following IDA solution for the current platform Windows Server 2003 R2:

- Active Directory directory services and Certificate Services—two core services that can be deployed separately or together.
- Authorization Manager, ADAM, and ADFS—separate optional components that require Active Directory directory services. (Authorization Manager also requires Certificate Services.)
- MIIS 2003, which is available both as a separate product or as a free Feature Pack (depending on whether or not you need to synchronize with non-Microsoft directory services).
- Windows Rights Management Service (RMS), which is available as an optional download from the Microsoft Download Center.

Microsoft's vision with Windows Server 2008 (and beyond) is to consolidate all these various IDA capabilities into a single, integrated IDA solution built upon Active Directory. This consolidation picture as of Beta 3 of Windows Server 2008 is as follows.

As shown in the following diagram, there are four key integrated IDA components present in Windows Server 2008:

- Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS), which provide the foundational directory services for domain-based and standalone network environments.
- Active Directory Certificate Services (AD CS), which provides strong credentials using PKI digital certificates.
- Active Directory Rights Management Services (AD RMS), which protects information contained in documents, e-mails, and so on.
- Active Directory Federation Services (AD FS), which eliminates the need for creating and maintaining multiple separate identities.



Note the following rebranding of IDA services in Windows Server 2008:

- Active Directory directory services is now known as Active Directory Domain Services (AD DS).
- Active Directory Application Mode is now called Active Directory Lightweight Directory Services (AD LDS).
- Certificate Services is now called Active Directory Certificate Services (AD CS).
- Windows Rights Management Services is now named Active Directory Rights Management Services (AD RMS).
- Finally, Active Directory Federation Services (ADFS) is still called Active Directory Federation Services (AD FS) but now includes an extra space in the abbreviation.

And for identity life-cycle management, Microsoft also plans on releasing a follow-up to MIIS 2003 called Identity Lifecycle Manager (ILM) 2007 in mid-2007. Initially, ILM 2007 will run on Windows Server 2003, Enterprise Edition. ILM 2007 builds on the metadirectory and user-provisioning capabilities in MIIS 2003 by adding new capabilities for managing strong credentials such as smart cards and by providing an integrated approach that pulls together metadirectory, digital certificate and password management, and user provisioning across Microsoft Windows platforms and other enterprise systems. Microsoft is also working on the next version of ILM, which is codenamed Identity Lifecycle Manager “2.” This version is planned for release around the same time as Windows Server 2008, but it will install separately. Before we go any further, let’s hear from one of our experts at Microsoft concerning plans for ILM “2” as an identity-management solution for Windows Server 2008:

From the Experts: Identity Lifecycle Manager “2”

Identity Lifecycle Manager “2” is the codename for Microsoft’s identity management solution for Windows Server 2008. The principles behind Identity Lifecycle Manager “2” are that identity is everywhere and it can be managed how you want it to be.

Identity Is Everywhere

Identity Lifecycle Manager “2” provides a plethora of ready-to-deploy self-service identity and access solutions. Users can manage their own information and that of their staff, and navigate through the organizational hierarchy. They can reset their own passwords, provision their own smart cards, and retrieve their certificates. They can create security groups and distribution lists, request access to one another’s groups, and manage approval.

Best of all, they can do all of this right from within their Office applications and Windows desktops. So, with Identity Lifecycle Manager “2,” if you want to request to join a group, you can do that right within Outlook. And when you are asked to approve an action by another user, the Approve and Reject buttons are right there in the approval request mail. And if you forget your password and need to reset it, you can do so right where you are most likely to find that you have forgotten it: at the Windows log-in prompt. All the facilities of Identity Lifecycle Manager “2” are also available from a central portal, hosted within Windows SharePoint Services.

Identity Is Managed How You Want It to Be

Identity Lifecycle Manager “2” lets you manage identity your way by allowing you to accurately model your business processes and attach them to identity and access events. Modeling your unique business procedures around identity and access management processes is meant to be something that each staff member can do for themselves, without having to depend on programmers to do it for them. Thus, Identity Lifecycle Manager “2” provides a simple graphical user interface for modeling your business procedures—the Identity Lifecycle Manager “2” Process Designer. Moreover, you don’t have to deploy any special software onto your user’s desktops for them to be able to use the Process Designer. The Process Designer is fully incorporated within the Identity Lifecycle Manager “2” portal, which is a Windows SharePoint Services 3 application. So all that users of the Process Designer need to access the designer is their browser.

The three fundamental types of processes that you can model in Microsoft Identity Lifecycle Manager “2” are authentication processes, approval processes, and action processes. Indeed, within Identity Lifecycle Manager “2,” processing proceeds by first executing your authentication processes, then your approval processes, and finally your action processes.

Authentication processes are for confirming a user’s identity. The steps in an authentication process challenge the user for credentials. This process can also include several steps to define a multifactor authentication process required for more

sensitive operations. Both the built-in authentication activities and your custom ones can leverage the Windows GINA and Windows Vista Credential Provider technologies to challenge users for their credentials at the Windows log-in prompt. This is a desirable option, because then users are challenged to prove their identity precisely where they expect to be challenged.

A second core type of process in the process model of Microsoft Identity Lifecycle Manager “2” is the approval process. Approval processes are for confirming that a user has permission to perform a requested operation. Typically, an approval process involves sending an e-mail message to the owner of a resource asking them to confirm that a user has permission to perform some requested operation on that resource. Identity Lifecycle Manager “2” allows users to respond to those approval requests right from within Outlook, which is precisely where a user would naturally want to be able to do so. Another type of activity in an approval process is one that requires users to submit a business justification for an operation they want to perform. In Identity Lifecycle Manager “2,” approval processes can involve any activities that a user might have to complete before being allowed to proceed with an operation. The enabling power of Identity Lifecycle Manager “2” is that it gives you the freedom to determine how you want to gather approvals for users’ actions. Then it surfaces the approvals on the end users’ desktops, inside an appropriate application context where they would expect to find them—saving the user from having to go elsewhere to manage permissions.

The third and final core type of process in the process model of Microsoft Identity Lifecycle Manager “2” is the action process. Action processes define what happens as a consequence of an operation. A simple example is just having a notification sent to the owner of a resource to inform the owner of a change. A more interesting and, indeed, more common type of activity to perform as a consequence of an identity management operation is an entitlement activity. Thus, you might define a process that, as a consequence of assigning a user to a particular group, allocates a parking permit in the correct lot and issues the appropriate card key for the user’s building. The point is that Identity Lifecycle Manager “2” action processes are truly a blank slate. On that blank slate, you get to define how actions on objects within Identity Lifecycle Manager “2” propagate out to the identity stores and resources of your enterprise.

We’ve said that the principal idea is that you get to define processes that model the identity management procedures of your enterprise and that you get to attach those processes to identity and access events. Up to this point, we have discussed quite a lot about the processes. Now let us turn to the subject of attaching those processes to events.

Events are the triggers that cause Identity Lifecycle Manager “2” processes to be executed. So, in attaching a process to an event, you are defining the circumstances under which the process will be executed. In the nomenclature of Identity Lifecycle Manager “2,” we refer to this as mapping a process to an event. We provide a simple user interface for accomplishing it. You identify the process that you have created using the Process Designer, and then you specify the event to which you want to attach the process.

So what is an *event* in Identity Lifecycle Manager “2?” Well, an event is something that happens to a set of one or more objects. For example, you might update the cost center assigned to a particular team of people, or you might update the office telephone number of a single individual. Both constitute examples of events. Another example is the addition of a person to a team—in that case, there is an event for the person being added, as well as an event for the team that the person is joining.

Because an event is something that happens to a set of one or more objects, when you map a process to an event, you must identify the set of objects to which the event is expected to occur. Identity Lifecycle Manager “2” gives you considerable power to identify the sets of objects. You get to define the rules by which objects are included in sets. Those rules can be as rich and complex or as bare and simple as you want them to be. You can define them so as to include any number of objects in a set, and any variety of types of objects as well. Once you have defined rules to identify a set of objects, you can select the events on those objects that you want to serve as triggers for your processes. There are two types of events in Identity Lifecycle Manager “2” that can trigger your processes: request events and transition events.

Request events are events by which the data of an object or set of objects is retrieved or manipulated. So, included in the category of request events are create, read, update, and delete events. Transition events occur when an object moves in or out of a set of objects. So, in the earlier example of a person joining a team, there is a transition for that person in being included in the group and a transition for the group in having that person join.

All in all, the authentication, approval, and action processes that you compose using approval actions, notification actions, and entitlement actions in the Process Designer can be mapped to any request or transition event on any set of objects that you identify via your rules. We believe that this simple model of designing processes and then mapping those processes to events gives you tremendous power to manage the identity life cycle of your organization. Whatever identity-related occurrences that you can imagine happening in your enterprise can be represented as events within Identity Lifecycle Manager “2,” and then you can describe processes to handle those events—processes that confirm the identity of the person initiating the event, that confirm the person’s permission to initiate the event, or that define the consequences. Crucially, you get to define

those processes as models representing the business policies and procedures that uniquely govern the identity-related assets of your enterprise.

Microsoft Identity Lifecycle Manager “2” is built on the Windows Communication Foundation, Windows Workflow Foundation, and Windows SharePoint Services 3 technologies, and it exposes a thoroughly standards-based API that implements WS-Transfer, WS-ResourceTransfer, WS-Enumeration, and WS-Trust.

–Donovan Follette

Identity and Access Developer Evangelist, Windows Server Evangelism

After reading all this, you hopefully understand now the big picture of what Microsoft’s vision is for identity and access, and how Active Directory in Windows Server 2008 fits into this picture. Now it’s time to look at each piece of this picture and learn about the new features and enhancements to Active Directory in Windows Server 2008. We’ll begin with core improvements to AD DS/LDS.

Active Directory Domain Services

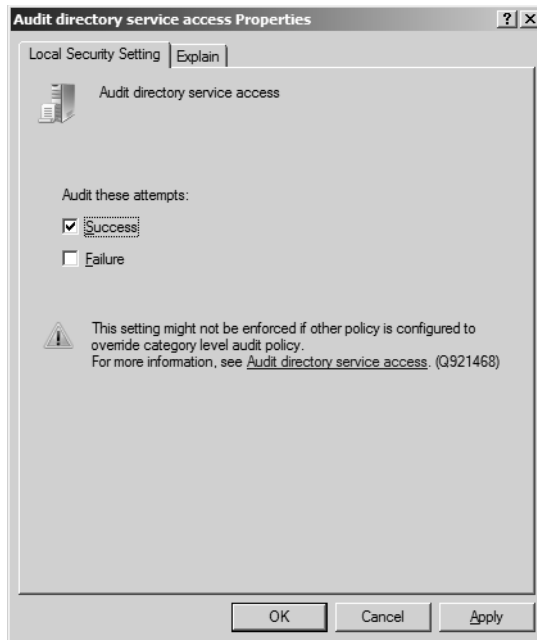
Let’s look at four enhancements to Active Directory in Windows Server 2008:

- AD DS auditing enhancements
- Read-only domain controllers
- Restartable AD DS
- Granular password and account lockout policies

There are other improvements as well, including some changes to the user interface for managing Active Directory and also to the Active Directory Installation Wizard. But we’ll focus here on the three enhancements just mentioned, as they’re big gains for many enterprises.

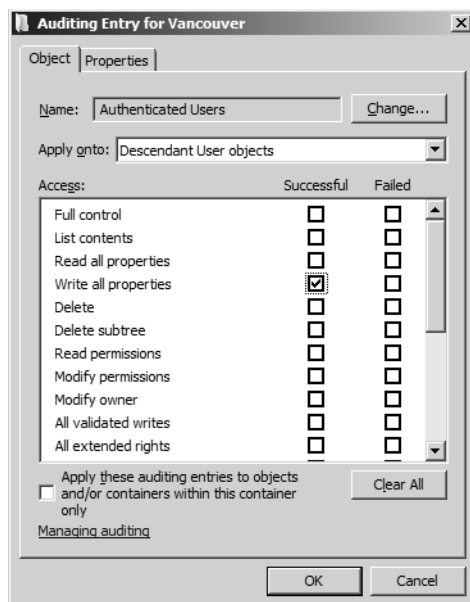
AD DS Auditing Enhancements

The first enhancement we’ll look at is AD DS auditing. In the current platform, Windows Server 2003 R2 (and in Windows Server 2008 also), you can enable a global audit policy called Audit Directory Service Access to log events in the Security event log whenever certain operations are performed on objects stored in Active Directory. Enabling logging of objects in Active Directory is a two-step process. First, you open the Default Domain Controller Policy in Group Policy Object Editor and enable the Audit Directory Service Access global audit policy found under Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy.

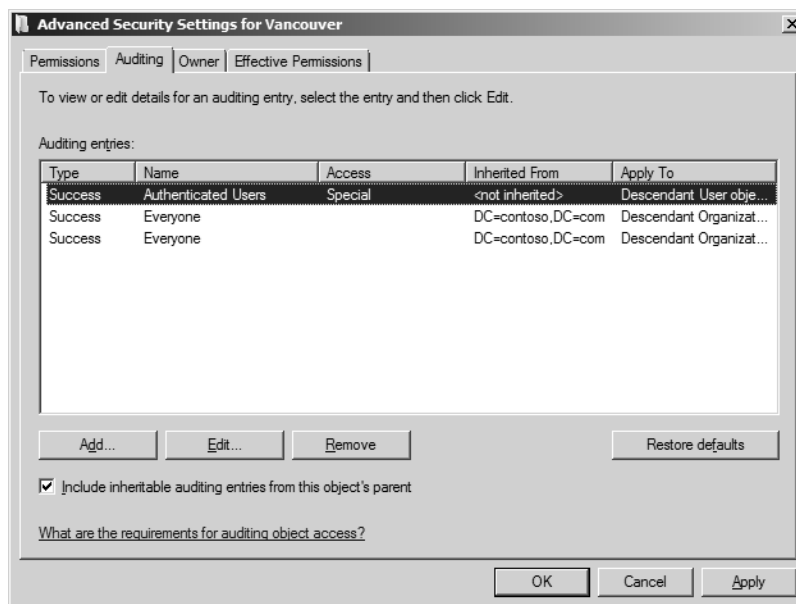


Then you configure the system access control list (SACL) on the object or objects you want to audit. For example, to enable Success auditing for access by Authenticated Users to User objects stored within an organizational unit (OU), you do the following:

1. Open Active Directory Users and Computers, and make sure Advanced Features is selected from the View menu.
2. Right-click on the OU you want to audit, and select Properties.
3. Select the Security tab, and click Advanced to open the Advanced Security Settings for the OU.
4. Select the Audit tab, and click Add to open the Select User, Computer or Group dialog.
5. Type **Authenticated Users**, and click OK. An Auditing Entry dialog opens for the OU.
6. In the Apply Onto list box, select Descendant User Objects.
7. Select the Write All Properties check box in the Select column.

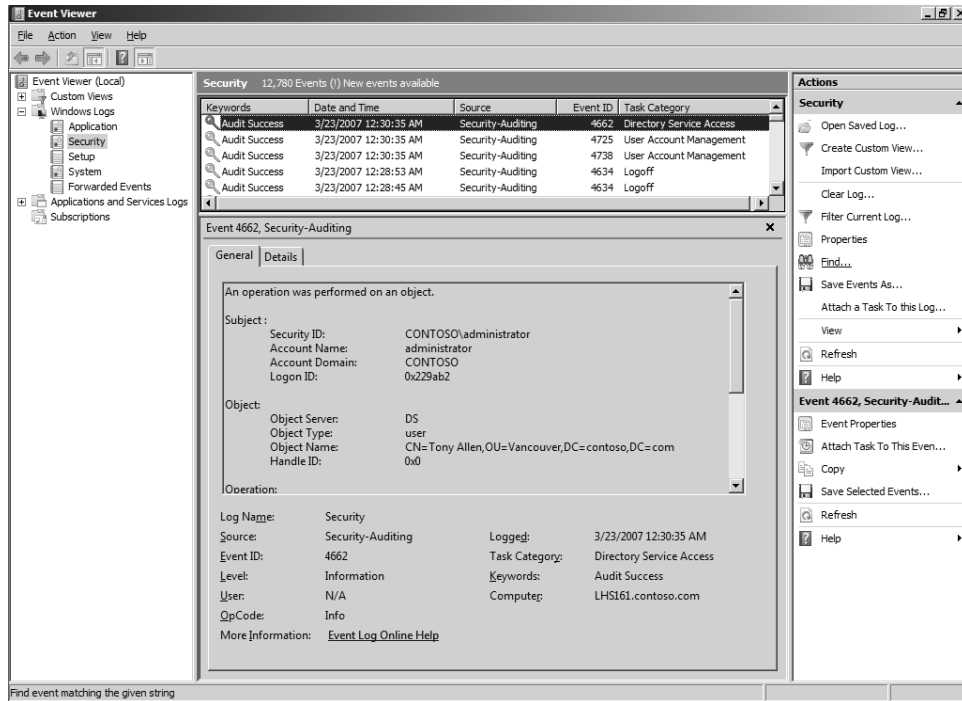


8. Click OK to return to Advanced Security Settings for the OU, which should now show the new SACL you configured.



9. Close all dialog boxes by clicking OK as needed.

Now if you go ahead and change a property of one of the user accounts in your OU—for example, by disabling an account—an event should be logged in the Security log with event ID 4662 and source Directory Service Access to indicate that the object was accessed.



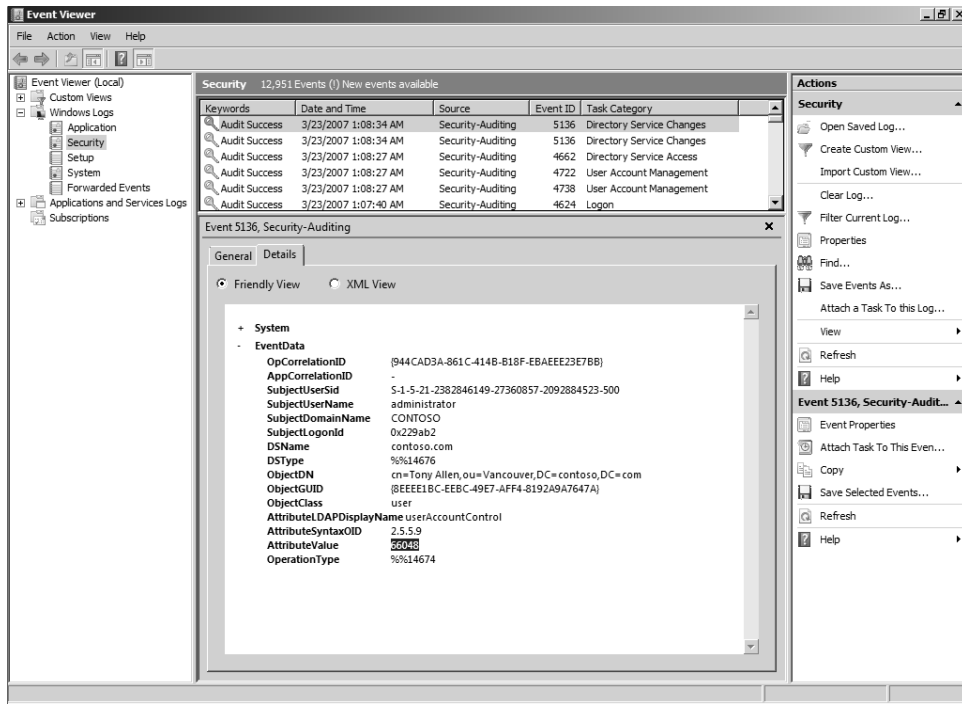
So far, this is the same in Windows Server 2008 as in previous versions of Windows Server. What's new in Windows Server 2008, however, is that while in previous Windows Server platforms there was only one audit policy (Audit Directory Service Access) that controlled whether auditing of directory service events was enabled or disabled, in Windows Server 2008 this policy has been divided into four different subcategories as follows:

- Directory Service Access
- Directory Service Changes
- Directory Service Replication
- Detailed Directory Service Replication

One of these subcategories—Directory Service Changes—has been enhanced to provide the ability to audit the following changes to AD DS objects whose SACLs have been configured to enable the objects to be audited:

- Objects that have had an attribute modified will log the old and new values of this attribute in the Security log.
- Objects that are newly created will have the values of their attributes at the time of creation logged in the Security log.
- Objects that are moved from one container to another within a domain will have their old and new locations logged in the Security log.
- Objects that are undeleted will have the location to which the object has been moved logged in the Security log.

The usefulness of this change should be obvious to administrators concerned about maintaining an audit trail of changes made to Active Directory, and auditing actions like these is an important part of an overall IDA strategy for an organization. For instance, using the Security log and filtering for a particular User object, you can now track in detail all changes to the attributes of that object over the entire lifetime of the object. When you enable Success auditing for the Audit Directory Service Access global audit policy (and this policy has Success auditing enabled for it by default within the Default Domain Controllers Policy), the effect of this is to also enable Success auditing for the first of the four subcategories (Directory Service Access) described earlier, which audits only attempts to access directory objects. If you need to, however, you can selectively enable or disable Success and/or Failure auditing for each of these four auditing subcategories individually by using the Auditpol.exe command-line tool included in Windows Server 2008. For example, if you wanted to enable Success auditing for the second subcategory (Directory Service Changes) so that you can maintain a record of the old and new values of an object's attribute when the value of that attribute is successfully modified, you can do so by typing **auditpol /set /subcategory:"directory service changes" /success:enable** at a command prompt on your domain controller. If we do this in the preceding example and then enable the user account we disabled previously, three new directory service audit events are added to the Security log.



The first (earliest) of these events is 4662, indicating the User object has been accessed, while the second event (5136) records the old value of the attribute modified and the third event (also 5136) records the new value of the attribute. Table 7-1 lists the possible event IDs for Directory Service Changes audit events.

Table 7-1 Event IDs for Directory Service Changes Audit Events

Event ID	Meaning
5136	An attribute of the object has been modified.
5137	The object was created.
5138	The object has been undeleted.
5139	The object has been moved within the domain.

In addition to enabling you to track the history of an object this way, Windows Server 2008 also gives you the option of setting flags in the Active Directory schema to specify which attributes of an object you want to track changes for and which attributes you don't want to track changes for. This can be very useful because tracking changes to objects can lead to a whole lot of audit events and your Security log can fill up awfully fast.

Read-Only Domain Controllers

Another new feature of AD DS in Windows Server 2008 is the Read-Only Domain Controller (RODC), a domain controller that hosts a read-only replica of the AD database. The main rationale for RODCs (apart from nostalgia for the BDCs of good old NT4 days) is to provide a solution for branch offices that have inadequate physical security. For example, a corporate headquarters probably has the resources to adequately protect their domain controllers against theft or other physical dangers—at least, they better have such resources. Small branch offices, however, might not have the facilities, budget, or expertise to ensure a domain controller present there would be physically secure. One solution to this problem might be to not have a domain controller at all at your branch office and just have users there authenticate over a WAN link with a domain controller at headquarters. The problem with this approach is if the WAN link is too slow, unreliable, or saturated with other forms of traffic. The result could be unacceptably slow logons for users or difficulty logging on at all. If your WAN link is unsuitable, the other option is to place a domain controller at your branch office and have users there authenticate locally while the DC itself replicates with DCs at headquarters to ensure its directory database is always up to date. The problem with *this* approach, however, is that domain controllers are the heart and soul of your Windows-based network because they contain all the accounts for all the users and computers on your network. So if the domain controller at your branch office somehow got stolen (perhaps by some clever social engineering like, “Hi, I’ve come to clean your domain controller, can you show me where it is?”), your whole network should be considered compromised and your only viable solution is to flatten everything and rebuild it all from scratch.

And those are the only two solutions today for branch offices using domain controllers running Windows Server 2003—authenticate over the WAN or risk placing a domain controller at your branch office. RODC, however, solves this dilemma by providing a *secure* way to have a domain controller at your branch office. The only requirement for using RODC is that the domain controller that holds the PDC Emulator FSMO role on your network has to be running Windows Server 2008. Once this is the case and you’ve deployed an RODC at your branch office, changes made to the directory on your normal (writable) domain controllers replicate to the RODC, but nothing replicates in the opposite direction. That’s because the directory database of a RODC is read-only, so you can’t write anything to it locally—it has to receive all changes to its database via replication from another (writable) domain controller. (RODCs can’t replicate with each other either, so there’s no point having more than one RODC at a given site—plus it could cause inconsistent logon experiences for users if you did do this.) So RODC replication is completely unidirectional—and this applies to DFS replication traffic as well.

RODCs also advertise themselves as the Key Distribution Center (KDC) for the branch office where they reside, so they handle all requests for Kerberos tickets from user and computer accounts at the remote site. RODCs don’t store user or computer credentials in their directory database, however; so when a user at the branch office tries to log on, the RODC contacts a

writable DC at the hub site to request a copy of the user's credentials. How the hub DC responds to the RDOC's request depends on how the Password Replication Policy is configured for that RDOC. If the policy says that the user's credentials can be replicated to the RDOC, the writable DC does this, and the RDOC caches the credentials for future use (until the user's credentials change). The result of all this is that RDOCs generally have few credentials stored on them. So if an RDOC somehow gets stolen (remember the DC cleaning guy), only those credentials are compromised and replacing them is much less work than rebuilding your entire directory from scratch.

Another feature of RDOCs is that a domain administrator can delegate the local administrator role for an RDOC to an ordinary domain user. This can be very useful for smaller branch offices that have no full-time expert IT person on site. So if you need to load a new driver into your DC at a remote site, you can just give instructions to your "admin" by phone on how to do this. The admin is simply an ordinary user who can follow instructions, and delegating RDOC admin rights to him doesn't enable him to perform any domain-wide administrative tasks or log on to a writable DC at headquarters—the damage he can do is limited to wrecking only the RDOC.

Let's hear now from a Microsoft MVP and directory services expert concerning some enhancements that have been made to `dcpromo.exe` in Windows Server 2008 and how these enhancements relate to deploying RDOCs:

From the Experts: New Active Directory Setup Wizard (dcpromo.exe)

When you want to install Active Directory, you have to use the Active Directory Setup Wizard (`dcpromo.exe`). It provides you with some possibilities and assumes that you have a proper design written down and you know what you want to accomplish. However, we have received many support calls and questions on the Internet because Active Directory and DNS were not set up in a way that reflects best practices. Considering the vast amount of installations of Active Directory, it's very clear that it's far easier to find the Active Directory Installation Wizard on the server operating system than it is to find best practices or good consultancy. Common support issues included having the wrong FSMO-Roles together on the same system, not enough Global Catalog servers, or issues in the DNS-Design that were leading to logons over the WAN lines.

In Windows Server 2008, Microsoft has put a huge effort into changing `dcpromo.exe`. Now it is reflecting best practices. You get a normal mode if you just want to quickly install Active Directory, and you get an advanced mode if you want to do any special configurations. `Dcpromo` is leveraging best practices, and it provides a lot of additional tasks. It's checking the FSMO roles for you, and it recommends whether to automatically move the Infrastructure Master if necessary. It allows you to enable the Global Catalog on a new domain controller. It is checking the DNS infrastructure, and it allows you to automatically create forwarders and delegations. Also, `dcpromo` enables you to choose

your replication partner for the initial replication so that you can make sure to target a specific DC.

In addition, dcpromo supports the new Read Only Domain Controller (RODC) in multiple ways. You are either able to precreate a RODC-Account in your domain and delegate a site admin to join the RODC to the domain, or you are able to fully install the RODC while selecting whether it should also be a Global Catalog server a DNS-server, or both.

Last but not least, dcpromo finally supports unattended installations from the command line without an answer script. Simply run **dcpromo /?:unattend** to figure out what parameters you have to script the installation of your Windows Server 2008 Active Directory Domain Controller.

–Ulf B. Simon-Weidner

MVP for Windows Server–Directory Services author, consultant, speaker, and trainer

Finally, because domain controllers often host the DNS Server role as well (because DNS is the naming system used by AD), the RODCs need a special read-only form of DNS Server running on them also. To learn more about this feature, however, let's listen to another one of our experts at Microsoft:

From the Experts: Advanced Considerations for DNS on RODCs in Branch Office Sites

When installing a Windows Server 2008 Read Only Domain Controller (RODC) at a branch office site, using the Active Directory Installation Wizard or the DCPromo command-line tool, you are prompted to specify a DNS domain for the Active Directory domain that you are joining the RODC to during promotion. During this process, you are prompted with DNS Server installation options. A DNS Server is required to locate domain controllers and member computers in an Active Directory domain, at both the hub site and the local branch office site. The default option is to install a DNS Server locally on the RODC, which replicates the existing AD-integrated zone for the domain specified and adds the local IP address in the DNS Server list of the domain controller local DNS Client setting.

As a best practice, Microsoft recommends that client computers have Dynamic DNS updates turned on by default and that DHCP Servers be used to configure the DNS Server list. Similarly for branch office sites, clients should be configured to use Dynamic DNS updates, and you should set the Primary DNS Server or use DHCP to set the DNS Server list to direct clients to the DNS Server running on the RODC.

If there is only one DNS Server and RODC running at the branch office site, Microsoft recommends that client computers also point to a DNS Server running on a domain controller at the hub site. This can be done either by configuring clients with an Alternate DNS Server for the hub-site DNS Server or by configuring DHCP Servers to set the DNS Server list to first the local DNS Server and then the remote DNS Server at the hub site. The DNS Server on the RODC should be the first DNS Server in the list to optimize resolution performance for branch office clients.

In larger branch office scenarios, if setting up two or more RODCs at a site, you are provided the default option to install DNS Server locally on all the RODCs. Within the same site, the RODCs do not replicate directly with each other. The RODCs rely mainly on replication with domain controllers at the hub site during scheduled intervals to refresh local data in the directory. Hence, a branch office DNS Server on an RODC receives updated DNS zone data during the normal replication cycle from a hub-site domain controller connected to the local RODC.

In addition to replication from the hub site, DNS Servers on RODCs also attempt to replicate local data after receiving a client update request. The branch office DNS Server redirects the client to a hub-site DNS Server on a domain controller that is writable and can process the update. Shortly thereafter, it attempts to contact a hub-site domain controller to update its local copy of the data with the changed record. Any other branch office DNS Server on RODCs at the site do not attempt to obtain a local copy of the single record update because they did not receive the original client update request. This mechanism has the advantage of allowing an updated client record to be resolved quickly within the branch office, without necessitating frequent and large replication requests for all domain data from the hub site. If network connectivity is lost, or no domain controller at the hub site is able to provide the updated record data to the DNS Server in the branch office, the record will be available locally only after the next scheduled replication from the hub-site domain controllers, and it will be available to all RODCs at the branch office site.

As a consequence of a DNS Server's attempt to replicate individual records between replication cycles, if DNS zone data is stored across multiple RODCs, the local branch office records might accumulate some incongruities. To ensure a high level of consistency for DNS data, the recommendation is to configure all client computers at the branch office site with the same DNS Server list—for example, by using DHCP.

If, however, in the more rare case that timely resolution of local branch office client records is absolutely critical, to avoid any inconsistencies for resolution, you can install DNS Servers on all RODCs at the site, but point clients only to a single DNS Server.

—Moon Majumdar

Program Manager, DNS (Server and Client) and DC Locator, Directory and Service Team

Restartable AD DS

Another new feature of AD DS in Windows Server 2008 is the ability to restart the Active Directory directory services without having to restart your domain controller in Directory Services Restore Mode. In previous versions of Windows Server, when you wanted to do some maintenance task on a domain controller—such as performing offline defragmentation of the directory database or performing an authoritative restore of the Active Directory directory service database—you had to restart your domain controller in Directory Services Restore Mode by pressing F8 during startup and selecting this from the list of startup options. You then logged on to your domain controller by using the local Administrator account specified previously when you ran the Active Directory Installation Wizard (dcpromo.exe) on your machine to promote it from a member server to a domain controller. Once logged on in Directory Services Restore Mode, you could perform maintenance on your domain controller and clients couldn't authenticate with it during your maintenance window.

Having to reboot a domain controller like this to perform maintenance operations resulted in longer downtime for clients who needed to be authenticated by your domain controller. To reduce this downtime window, AD DS has been re-architected in Windows Server 2008. Instead of rebooting your machine and logging on in Directory Services Restore Mode, you simply stop the Domain Controller service by using the Services snap-in (shown in Figure 7-1) or typing **net stop ntlds** at a command line, perform your maintenance tasks while still logged on as a domain admin, and when you're finished start this service again using the snap-in or the **net start ntlds** command. Stopping and starting the Domain Controller service like this also has no effect on other services such as the DHCP Server service that might be running on your domain controller.

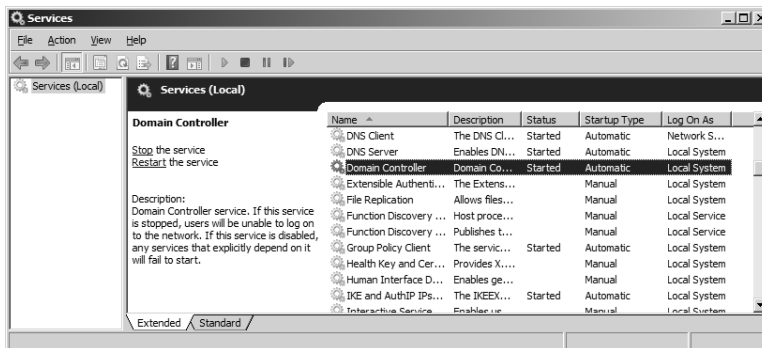


Figure 7-1 You can now stop and start the Domain Controller (NTDS) service without rebooting your domain controller and logging on in Directory Services Restore Mode

While domain controllers running previous versions of Windows Server had two Active Directory directory service modes (normal mode and Directory Services Restore Mode), domain controllers running Windows Server 2008 now have three possible modes or *states* they can be running in:

- **AD DS Started** This is the normal state when the NTDS service is running and clients can be authenticated by the domain controller. This state is similar to how AD directory services worked in Windows 2000 Server and Windows Server 2003.
- **Directory Services Restore Mode** This state is still available on domain controllers running Windows Server 2008 through the F8 startup options, and it's unchanged from how it worked in Windows 2000 Server and Windows Server 2003.
- **AD DS Stopped** This is the new state for domain controllers running Windows Server 2008. A domain controller running in this state shares characteristics of both a domain controller running in Directory Services Restore Mode and a member server that is joined to a domain. For example, as in Directory Services Restore Mode, a domain controller running in the AD DS Stopped state has its directory database (Ntds.dit) offline. And similar to a domain-joined member server, a domain controller running in this state is still domain-joined, and users can log on interactively or over the network by using another domain controller. But it's a good idea not to let your domain controller remain in the AD DS Stopped state for an extended period of time because not only will it be unable to service user logon requests, it also will be unable to replicate with other domain controllers on the network.

Granular Password and Account Lockout Policies

New in Beta 3 of Windows Server 2008 is the ability to have multiple password policies and account lockout policies in a domain. To learn about this particular feature, let's hear from a Microsoft MVP and directory services expert:

From the Experts: Granular Password Policies in Windows Server 2008

If you want to deploy multiple password policies in your forest, the domain has always been the boundary for this. This was confusing for many customers because you are able to change passwords in every Group Policy Object (GPO). However, remember that password settings (and account lockout settings) are configured in the Computer Settings part of the GPO. They apply only to computer objects, and therefore, to local accounts on those computer objects. An exception to this rule is policies that are linked to the domain head (the top node of the domain). GPOs linked here that hold password

settings are the administrative interface for the password and account lockout settings for domain objects. Actually, they are written back to attributes on the domain head object and take effect from there. Domain controllers that receive a password change request compare the settings on the domain head with the password, and they either allow the password change or deny it. So it's important to understand that password and account lockout settings are maintained on the domain head in Active Directory. You also need to keep in mind that Group Policies are only the administrative interface and that password settings configured in any GPO linked to any other OU or site are applied only to the local user accounts of the computer object to which the policy applies.

So, in the past, password and account lockout settings were limited to the domain and we were able to apply only one setting per domain. If we wanted to have different password policies, we were required to deploy multiple domains.

This has been changed in Windows Server 2008. Active Directory is extended, and the password settings validation on the domain controllers have been extended so that we are able to configure multiple password and account lockout settings for each domain now. How are they administered? Not via GPO—as mentioned before, GPO has been only an administrative interface. So the new fine-grained password policies are configured as new objects in the domain and are linked to either groups or users in the domain.

If you want to experiment with this, simply use ADSIEdit.msc. Expand the Password Settings Container underneath the System Container in the domain, right-click, and select New. You are prompted to fill in the following mandatory attributes, which define password and account lockout policies:

- *msDS-PasswordSettingsPrecendence* This attribute is just a virtual number you can make up. (Be sure you leave some space in the numbering for future use.) It defines which password settings take effect if multiple settings apply to the same object (user or group, but settings on the user always take precedence over settings on the group).

This will usually reflect on the “level” of the settings object. For example, if you have stronger settings, they have a lower value, and if you have higher settings, you’re probably assigning a higher precedence to them.

- *msDS-PasswordReversibleEncryptionEnabled* This attribute is Boolean and defines whether you want to store the passwords of the accounts (that is, specify to whom the password settings object applies) in reversible encryption or not. The default and best practice is to set this value to FALSE.
- *msDS-PasswordHistoryLength* This setting defines how many old passwords the user cannot reuse again (to prevent the user from changing the password back and forward to the same one or changing it multiple times until he’s able to reuse his old password).

The domain default is to not allow the last 24 passwords of that user.

- *msDS-PasswordComplexityEnabled* This attribute is also a Boolean and defines whether the password needs to be complex (that is, it has at least three of the following character sets applied: lower letters, capital letters, numbers, symbols, or unicode characters).

The domain default and best practice is to turn it on (TRUE).

- *msDS-MinimumPasswordLength* This attribute defines the minimum length of a password in characters. The domain default is seven characters long.
- *msDS-MinimumPasswordAge* The *msDS-MinimumPasswordAge* attribute does just what its name suggests—it defines the minimum age for passwords. The minimum age is necessary to prevent a user from changing her password x amount of times on the same day until she exceeds the Password History limit and can change the password back to the same value as before.

This is a negative number that you can compile or decompile, using the scripts at <http://msdn2.microsoft.com/en-us/library/ms974598.aspx> as a guideline. (The domain default is 1 day, which equals -864000000000.)

- *msDS-MaximumPasswordAge* This attribute is just the opposite of the previous one. It defines when you have to change your password. It is also a negative number just like the previous one. (The domain default is 42 days, which equals -36288000000000.)
- *msDS-LockoutThreshold* Defines how many failed attempts at entering a password a user can have before the user object will be locked. (The domain default is 0, which equals “Don’t lock out accounts after invalid passwords.”)
- *msDS-LockoutObservationWindow* This attribute determines at which time the bad password counter should be reset. (The domain default is 6 minutes, which equals -18000000000.)
- *msDS-LockoutDuration* This attribute determines how long a password should be locked. (The domain default is 6 minutes, which equals -18000000000.)

After you create your own password settings object (PSO), you have to link it to a user or group. I recommend, for administrative purposes, always linking it to groups instead of to users. (Otherwise, it will get messy and hard to administer.) To link the PSO to a group or user, you simply change its *msDS-PSOAppliesTo* attribute to the distinguished name of the group or user (for example, *cn=Administrators,cn=Users,dc=example,dc=com*). This is a multivalued attribute, so you are able to link the same PSO to multiple groups or users.

For administrative purposes, there are also two attributes that help you determine which password policies are applied to which users or groups. On the group or user, you will find the *msDS-PSOApplied* attribute, which is actually the back link of the *msDS-PSOAppliesTo* attribute and lists all PSOs that are directly linked to this object.

To help you figure out which PSO is the effective one, there's the constructed attribute *msDS-ResultantPSO*, which shows you which PSO is effective for the object in question.

At the beta stage that is current at the writing of this book, this is a new feature that lacks adequate administrative support in the graphical user interface. However, you are able to administer it easily using *ADSIEdit.msc*. And Joe Richards, a Directory Services MVP who wrote Active Directory command line tools such as *ADFind* and *ADMod*, has created a new command-line utility named *PSOMgr.exe*, which helps you create and link PSOs. You'll find it at www.joeware.net.

—Ulf B. Simon-Weidner

MVP for Windows Server—Directory Services author, consultant, speaker, and trainer

Active Directory Lightweight Directory Services

Another feature of Active Directory in Windows Server 2008 is the new built-in Active Directory Lightweight Directory Services (AD LDS) server role. Well, actually it's not new because this is essentially the same Active Directory Application Mode (ADAM) feature that was available as an out-of-band download for Windows Server 2003 and Windows XP. What's new is mainly that this directory service is now available as an in-box role that can be added to your Windows Server 2008 server using the Role Manager tool described in Chapter 4, "Managing Windows Server 2008," instead of it needing to be downloaded from the Microsoft Download Center as in previous versions of Windows.

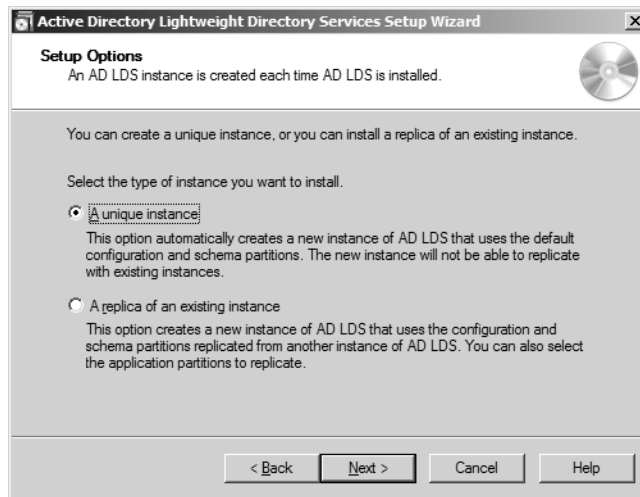
So AD LDS is basically just ADAM, but what's ADAM? ADAM (we'll call it by its new name now, AD LDS) is basically a stripped-down version of AD DS that supports a lot of the features of AD DS (multimaster replication, application directory partitions, LDAP over SSL access, the ADSI API) but doesn't store Windows security principals (such as domain user and computer accounts), domains, global catalogs, or Group Policy. In other words, AD LDS gives you all the benefits of having a directory but none of the features for managing resources on a network. Instead, AD LDS is designed to support applications that need a directory for storing their configuration and data instead of storing these in a database, flat file, or other form of repository. Examples of directory-enabled LOB apps that could use AD LDS include CRM and HR applications or global address book apps. Because such apps often require schema changes in order to work with AD DS, a big advantage of AD LDS is that you can avoid having to make such changes to your AD DS schema, as making mistakes when you modify your AD DS schema can be costly—think flatten and rebuild everything from scratch! And it's particularly useful also if your directory-enabled LOB apps will be made available to customers or partners over an extranet or VPN connection because using AD LDS instead of AD DS in this scenario means you don't have to risk exposing your domain directory to nondomain users and computers.

Once you've added the AD LDS role in Server Manager, to use this feature you create an AD LDS instance. An AD LDS instance is an application directory that is independent of your

domain-based AD DS and can run on either a member server or a domain controller if desired. (There's no conflict when running AD DS and AD LDS on the same machine as long as the two directories use a different LDAP path and different LDAP/SSL ports for accessing them. And you can even run multiple AD LDS instances on a single machine—for example, one instance for each LOB app on the machine—without conflict as long as their paths and ports are unique.)

Let's quickly walk through creating a new AD LDS instance and show how you can manage it:

1. After installing the AD LDS role on your server, select the Active Directory Lightweight Directory Services Setup Wizard from Administrative Tools on your Start menu. This launches a wizard for creating a new instance of AD LDS on the machine:



2. Select the A Unique Instance option, and click Next. Then specify a name for the new instance (using only alphanumeric characters and the dash in your name):



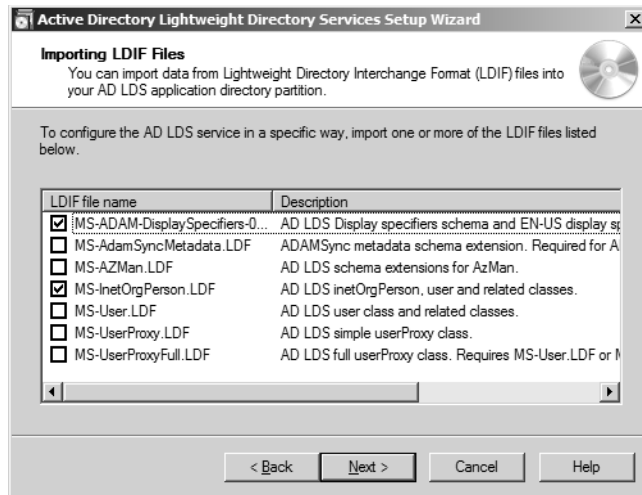
3. Click Next, and specify LDAP and SSL ports for accessing your instance:



4. Click Next, and either allow the application to create its own directory partition when you install the application or type a unique distinguished name (DN) for the new application partition you are going to create:



5. Click Next, and in the following wizard pages specify the location where data and recovery files for the partition will be stored, the service account under whose context the AD LDS instance will be running, and the user or group who will have administrative privileges for managing your instance. After completing these steps, you'll be asked to select from a list of default LDIF files you can import to add specific functionality to your instance:

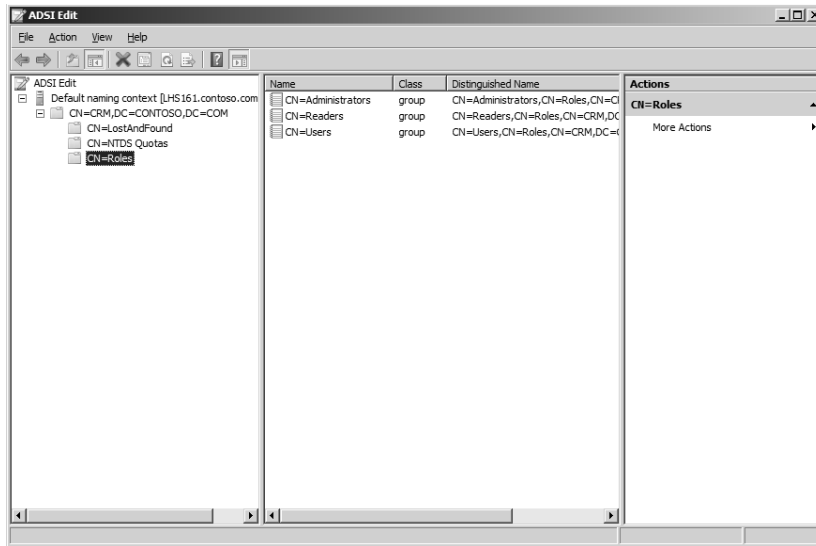


- Click Next to confirm your selections, and then click Finish to run the wizard and create the instance.

Once you've created your new AD LDS instance, you can manage it using ADSI Edit, an MMC snap-in available from Active Directory Lightweight Directory Services under Administrative Tools. To do this, open ADSI Edit, right-click on the root node, and select Connect To. When the Connection Settings dialog opens, specify the DN for the connection point to your instance (which was CN=CRM,DC=CONTOSO,DC=COM in our example) and click the Advanced button to specify the LDAP port (50000 in our example) for connecting to the instance:



Clicking OK then opens your AD LDS instance in ADSI EDIT. Then you can navigate the directory tree and view and create or modify objects and their attributes in your application directory partition as needed to support the functionality of your directory-enabled LOB app.



Active Directory Certificate Services

Let's move on and briefly describe improvements to Active Directory Certificate Services (AD CS) in Windows Server 2008. We'll focus on the following key improvements:

- Improvements to certificate Web enrollment support
- Support for Network Device Enrollment Service to allow network devices such as routers to enroll for X.509 certificates
- Support for the Online Certificate Status Protocol to easily manage and distribute certificate revocation status info
- The inclusion of PKIView for monitoring the health of Certification Authorities (CAs)

There are other improvements as well for AD CS—such as new Group Policy settings—but we'll pass over these for now because they'll be well documented once Windows Server 2008 RTMs. But we will also hear from the AD CS product group concerning some other enhancements to AC CS in Windows Server 2008.

Certificate Web Enrollment Improvements

Enrollment is the process of issuing and renewing X.509 certificates to users and computers when a PKI has been deployed in your enterprise. Users and computers belonging to an Active Directory domain can take advantage of a mechanism called *autoenrollment*, which

allows them to automatically enroll domain-joined computers when they boot and domain users when they log on. Windows Server 2003 also includes a Certificate Request Wizard to enable domain users to request a new certificate manually when they need to.

Users and computers that are not domain joined or that run a non-Microsoft operating system can use Web enrollment instead. Web enrollment is built on top of Internet Information Services and allows a user to use a Web page to request a new certificate or renew an existing one over an Internet or extranet connection.

What's changed with this feature in Windows Server 2008 is that the old XEnroll.dll ActiveX control for the Web enrollment Web application has now been retired for both security and manageability reasons. In its place, a new COM control named CertEnroll.dll is now used, which is more secure than the old control but whose use can pose some compatibility issues in a mixed environment. For reasons of time, we can't get into these compatibility issues here, but see the "Additional Resources" section at the end of this chapter for more information on this topic.

Network Device Enrollment Service Support

Another enhancement in AD CS in Windows Server 2008 is the inclusion of built-in support for the Network Device Enrollment Service (NDES). Let's listen to one of our experts at Microsoft briefly describe this new feature (and see the "Additional Resources" section at the end of the chapter for links to more information on the subject):

From the Experts: Network Device Enrollment Service

Network Device Enrollment Service is one of the optional components of the Active Directory Certificate Services (AD CS) role. This service implements the Simple Certificate Enrollment Protocol (SCEP). SCEP defines the communication between network devices and a Registration Authority (RA) for certificate enrollment.

SCEP enables network devices that cannot authenticate to enroll for x.509 certificates from a Certification Authority (CA). At the end of the transactions defined in this protocol, the network device will have a private key and associated certificate that are issued by a CA. Applications on the device can use the key and its associated certificate to interact with other entities on the network. The most common usage of this certificate on a network device is to authenticate the device in an IPSec session.

—Oded Shekel

Program Manager, Windows Security

Online Certificate Status Protocol Support

Another new feature of AD CS in Windows Server 2008 is support for the Online Certificate Status Protocol (OCSP). In a traditional PKI, such as one implemented using Certificate

Services in Windows Server 2003, certificate revocation is handled by using certificate revocation lists (CRLs). There has to be a way of revoking certificates that expire or are compromised; otherwise, a PKI system won't be secure. CRLs provide a way of doing this by enabling clients to download a list of revoked certificates from a CA to ensure the certificate they're trying to verify (for example, a certificate belonging to a server the client is trying to connect to) is valid. Unfortunately, once a lot of certificates have been revoked in an enterprise, the CRL can become quite large and have an impact on performance when authenticating over slow WAN links or during peak traffic times, like the beginning of the workday when everyone is trying to log on to the network at the same time.

To improve performance in checking for revoked certificates and increase the scalability of a PKI system, Windows Server 2008 includes an optional Online Certificate Status Protocol role service you can install on a server by adding the Active Directory Certificate Services role using Server Manager. OCSP provides an Online Responder that can receive a request to check for revocation of a certificate without the client having to download the entire CRL. This speeds up certificate revocation checking and reduces the network bandwidth used for this process, which can be especially helpful when such checking is done over slow WAN links. AD CS in Windows Server 2008 even supports *Responder* arrays, in which multiple OCSP Online Responders are linked together to provide fault tolerance, increased scalability, or functionality needed for geographically dispersed PKI deployments.

OCSP support is described in more detail in one of the links in the "Additional Resources" section at the end of this chapter. Meanwhile, let's hear from one of our experts at Microsoft concerning this new feature:

From the Experts: Online Responder

The Online Responder server rule implements the server component of the Online Certificate Status Protocol (OCSP).

OCSP uses Hypertext Transfer Protocol (HTTP) and allows a relying party to submit a certificate status request to an OCSP responder. This returns a definitive, digitally signed response indicating the certificate status. The Microsoft Online Responder was built with scalability, performance, security, and manageability in mind. It includes the following two components:

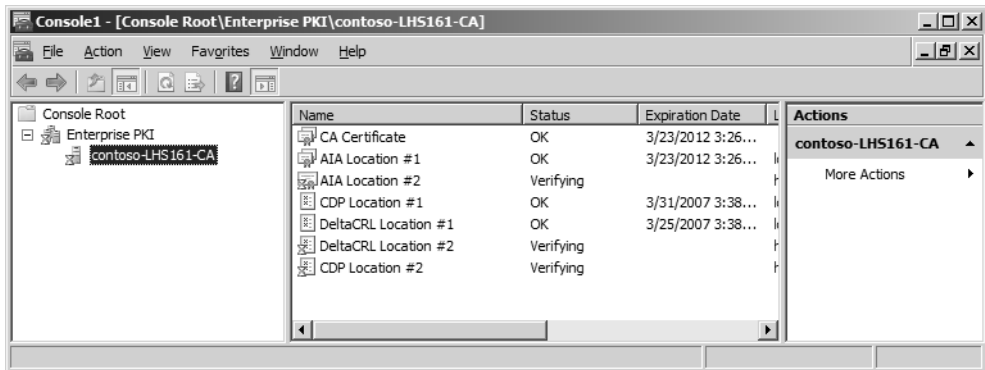
- **Online Responder Web Proxy Cache** First and foremost, this component is the service interface for the Online Responder. It is implemented as an Internet Server API (ISAPI) Extension hosted by Microsoft Windows Internet Information Services (IIS).
- **Online Responder Service** This component is a Microsoft Windows NT service (ocspvc.exe) that is running with NETWORK SERVICE privileges.

—Oded Shekel

Program Manager, Windows Security

Enterprise PKI and CAPI2 Diagnostics

Monitoring the health of CAs in an enterprise PKI deployment is important to prevent problems from arising and to troubleshoot issues when they arise. The Windows Server 2003 Resource Kit included a tool called PKI Health that could be used to display the status of each CA in a chain of CAs; in Windows Server 2008, this tool has been renamed Enterprise PKI (PKIView) and has been re-implemented as an MMC snap-in. Using PKIView, enterprise PKI admins can check the validity or accessibility status of authority information access (AIA) locations and certificate revocation list (CRL) distribution points (CDPs) for multiple CAs within an enterprise that has a Windows Server-based PKI deployed:



PKIView isn't the only way of troubleshooting problems with a Windows Server 2008-based PKI, however. Another useful tool is CAPI2 Diagnostics, which is described in the next sidebar contributed by one of our experts:

From the Experts: Troubleshooting PKI Problems on Windows Vista and Windows Server 2008

Microsoft Windows Vista and Microsoft Windows Server 2008 have a new feature—CAPI2 Diagnostics—that can help you with PKI troubleshooting. This feature enables administrators to troubleshoot PKI problems by collecting detailed information about certificate chain validation, certificate store operations, and signature verification. In case of errors in PKI-enabled applications, detailed information—such as the low-level API results and errors, objects retrieved, and status flags raised at different steps—is available in the logs. This functionality can help reduce the time required to diagnose problems. For troubleshooting purposes, enable CAPI2 logging, reproduce the problem, and use the data in the logs to identify the root cause. To enable logging, follow these steps:

1. Open the Event Viewer, and go to Application And Services Logs\Microsoft\Windows\CAPI2 to get the CAPI2 channel.

2. Right-click Operational, and select Enable Log to enable CAPI2 Diagnostics logging.
3. To save the log to a file, right-click Operational and select the Save Events As option. You can save the log file in the .evtx format (which can be opened through the Event Viewer) or in XML format.
4. If there is data present in the logs before you reproduce the problem, it is recommended that you clear the logs before the repro. This allows only the data relevant to the problem to be collected from the saved logs. To clear the logs, right-click Operational and select the Clear Log option.
5. The default size for the event log is 1 MB. For CAPI2 Diagnostics, the logs tend to grow in size quickly, and it is recommended that you increase the log size to at least 4 MB to capture relevant events. To increase the log size, right-click Operational and select the Properties option. In the log properties, increase the maximum log size.

To learn more about CAPI2 Diagnostics, check out the whitepaper titled “Troubleshooting PKI Problems on Windows Vista” at <http://www.microsoft.com/downloads/details.aspx?FamilyID=FE8EB7EA-68DA-4331-9D38-BDBF9FA2C266&displaylang=en>.

–Yogesh Mehta

Program Manager, Windows Security

Other AD CS Enhancements

Finally, let’s briefly hear from one of our experts on the product team at Microsoft concerning two more enhancements to AD CS in Windows Server 2008. Our first sidebar outlines some important changes to V3 certificate templates and the cryptographic algorithms they support in Windows Server 2008 (and in Windows Vista):

From the Experts: V3 Certificate Templates

One important change in Windows Server 2008 and Windows Vista is the support for CNG (Suite-B). With Suite-B algorithms, it is possible to use alternate and customized cryptographic algorithms for encryption and signing certificates.

To support these algorithms, a new certificate template version was added—V3. A V3 certificate template is enhanced in the following ways:

- Support for asymmetric algorithms implemented by a Key Service Provider (KSP) for CNG. By default, Windows implements the following algorithms: DSA, ECDH_P256, ECDH_P384, ECDH_P521, ECDSA_P256, ECDSA_P384, ECDSA_P521, and RSA.

- Support for hash algorithms implemented by a KSP. By default, Windows implements the following algorithms: MD2, MD4, MD5, SHA1, SHA256, SHA384, and SHA512.
- A discrete signature (PKCS#1 V2.1) can be required for certificate requests. Activating this option forces a client that uses the certificate autoenrollment functionality or enrolls a certificate through the Certificates MMC snap-in to generate a certificate request that carries a discrete signature. Selecting this option does not mean that a certificate that is issued from this template also carries a discrete signature. The setting applies to the certificate request only. Also, the setting is not relevant for certificate requests that are created with the `certreq.exe` command-line tool.
- The Advanced Encryption Standard (AES) algorithm can be specified to encrypt private keys while they are transferred to the CA.
- For machine templates, read permissions on the private key can be added to the Network Service so that services such as IIS have permission to use certificates and keys that are available in the computer's certificate store. In previous versions of Windows, manually adjusting permissions on the computer's certificate store is required.
- The list of asymmetric algorithms is filtered based on the template purpose in the Request Handling tab.

—Oded Shekel

Program Manager, Windows Security

And our second sidebar describes the new restricted enrollment agent functionality in Windows Server 2008's implementation of Enterprise CA:

From the Experts: Restricted Enrollment Agent

Enrollment agents are one or more authorized individuals within an organization. The enrollment agent needs to be issued an Enrollment Agent certificate, which enables the agent to enroll for certificates on behalf of users. Enrollment agents are typically members of the corporate security, IT security, or help desk teams because these individuals have already been trusted with safeguarding valuable resources. In some organizations, such as banks that have many branches, help desk and security workers might not be conveniently located to perform this task. In this case, designating a branch manager or other trusted employee to act as an enrollment agent is required.

The Windows Server 2003 Enterprise CA does not provide any configurable means to control enrollment agents except from enrollment agents' certificates enforcement. The enrollment agent certificate is a certificate containing the Certificate Request Agent application policy extension (OID=1.3.6.1.4.1.311.20.2.1).

The restricted enrollment agent is a new functionality that allows limiting the permissions that enrollment agents have for enrolling on behalf of other users. On a Windows Server 2008 Enterprise CA, an enrollment agent can be permitted for one or many certificate templates. For each certificate template, you can configure which users or security groups the enrollment agent can enroll on behalf of. You cannot constrain an enrollment agent based on a certain Active Directory organizational unit (OU) or container. As mentioned previously, you must use security groups. Note that the restricted Enterprise enrollment agent is not available on a Standard CA.

—Oded Shekel

Program Manager, Windows Security

Active Directory Federation Services

Active Directory Federation Services (AD FS) is another important part of the overall IDA solution provided by Windows Server 2008. AD FS is designed to address a situation that is common in business nowadays—a partner or client that resides on a different network has to access a Web application exposed by your own organization's extranet. In a typical scenario, the client has to enter secondary credentials to this when she tries to access a Web page on your extranet. That's because the client's credentials on her own network might not be compatible or might not even be known by the directory service running on your own network.

AD FS is designed to eliminate the need for entering such secondary credentials by providing a mechanism for supporting single sign-on (SSO) between different directories running on different networks. AD FS does this by providing the ability to create trust relationships between the two directories that can be used to project a client's identity and access rights from her own network to networks belonging to trusted business partners. By deploying one or more federation servers in multiple organizations, federated business-to-business (B2B) partnerships can also be established to facilitate B2B transactions between trusted partners.

To deploy AD FS, at least one of the networks involved must be running either AD DS or AD LDS. AD FS has been around since Windows Server 2003 R2, but it has been enhanced in several ways in Windows Server 2008. For example, AD FS is now easier to install and configure in Windows Server 2008 because it can be added as a server role using Server Manager. AD FS is also easier to administer in Windows Server 2008, and the process of setting up a federated trust between two organizations by exporting and importing policy files is now simpler and more robust. Finally, AD FS now includes improved application support and is more tightly integrated with Microsoft Office SharePoint Services 2007 and also the Active Directory Rights Management Services (AD RMS) component of Windows Server 2008.

Let's learn some more about the improved import/export functionality in AD FS in Windows Server 2008 from some of our product group experts:

From the Experts: Using Import/Export Functionality to More Efficiently Create Federation Trusts

There's no doubt about it. Setting up a federation trust between two organizations can be a daunting task because of the many sequential steps involved in manually setting up both partners for successful AD FS communications. In this scenario, both administrators are equally responsible for entering in values and addresses (that is, URIs, URLs, and claims) within the AD FS snap-in that are unique to their company's federation environment.

Once this initial setup phase has been completed, each administrator must then provide these values to the administrator in the other organization so that a federation trust can be properly established. Even when these values are sent to the intended partner administrator, there is the distinct possibility that an administrator can accidentally type in a value incorrectly and inadvertently cause himself or herself many hours of headaches trying to locate the source of the problem with the new trust.

In Windows Server 2008, improvements have been made that allow partner administrators to export their generic trust policy and partner trust policy into a small xml file format that can easily be forwarded via e-mail to a partner administrator in another organization. The generic trust policy contains the Federation Server Display Name, URI, Federation Server Proxy URL, and any verification certificate information; whereas the partner trust policy file also includes information about each of the claims. With this in mind, the second-half of the federation trust can then be quickly established by importing the partner's trust policy and mapping the claims.

This "export and e-mail" process adds the following benefits for the partner administrator who receives the xml file:

- Expedites the process of establishing a federation trust because the administrator can choose to import the contents of the xml file in the Add Partner Wizard and simply click through the wizard pages to verify that the imported settings are suitable
- Eliminates the additional step of importing the account verification certificate because the import process does this automatically
- Provides for easy claim mapping
- Eliminates the possibility of manual typing errors

You can test-drive this new functionality by walking through the Windows Server 2008 version of the AD FS Step-by-Step Guide.

—Nick Pierson

Technical Writer of CSD (Connected System Division) UA team

—Lu Zhao

Program Manager, Active Directory Federation Service

—Aurash Behbahani

Software Design Engineer, Active Directory Federation Service

Another new feature of AD FS in Windows Server 2008 is the ability to use Group Policy to prevent setting up unauthorized federation servers in your domain. Here's how some of our experts at Microsoft describe this enhancement:

From the Experts: Limiting Federation Service Deployment Using Group Policy

In Windows Server 2003 R2, AD FS did not provide control mechanisms that prevented users from installing or configuring their own federation service. In Windows Server 2008, AD FS administrators can now turn on Group Policy settings that prevent unauthorized federation servers in their domain. This new setting helps to satisfy the needs of an IT department when they want to enforce compliance or legal process requirements.

Once the Group Policy setting has been enabled, the value *DisallowFederationService* is inserted into the registry key on each federation server in that domain. Before an AD DS domain-joined computer running the Windows Server 2008 operating system can install the Federation Service server role, the server first checks to make sure that the Don't Allow Non-authorized Federation Servers In This Domain Group Policy setting is enabled. If this setting is enabled, the installation of the Federation Service will fail. If it is not enabled, which is the default setting, installation of a Federation Service will be allowed and the installed Federation Service will function normally.

The registry key value is checked only when the trust policy file is loaded, so there might be a delay between when the update appears that brings down the policy and when the Federation Service observes the policy. By default, the policy is read when a file change notification is received and also once every hour.

Note that this feature applies only to Windows Server 2008 federation servers and does not affect new or existing installations of a Federation Service in Windows Server 2003 R2.

–Lu Zhao

Program Manager, Active Directory Federation Service

–Nick Pierson

Technical Writer of CSD (Connected System Division) UA team

Finally, AD FS can be integrated with AD CS, but when problems occur with this scenario you need to know how to troubleshoot them. Here are some more of our experts explaining how to do this:

From the Experts: Troubleshooting Certificate Revocation Issues

Certificate issues are among the top five AD FS troubleshooting hot spots for the product support team here at Microsoft. One particular AD FS-related certificate issue centers on a known routine process that checks for the validity of a certificate by comparing it to a CA-issued list of revoked certificates. This process, in the world of PKI, is known as certificate revocation list (CRL) checking.

The revocation verification setting configured for an account partner on a federation server is used by the federation server to determine how revocation verification will be performed for tokens sent by that account partner. The revocation verification setting of the federation server itself, configured on the Trust Policy node of the AD FS snap-in, is used by the federation server and by any AD FS Web agent bound to the federation server to determine how the revocation verification process will be performed for the federation server's own token signing certificate. The verification process will make use of CRLs imported on the local machine or that are available through the CRL Distribution Point.

When troubleshooting certificate issues, it is important to be able to quickly disable revocation checking to help you locate the source of the problem. For example, this can be helpful in deployment scenarios where there are no CRLs available for the token-signing certificates.

To help troubleshoot CRL-checking issues, the AD FS product team has provided a method within the AD FS snap-in in Windows Server 2008 where you can adjust or disable how revocation checking behaves within the scope of a federation service. For example, you can set revocation checking to check for the validity of all the certificates in a certificate chain or only the end certificate in the certificate chain.

–Nick Pierson

Technical Writer of CSD (Connected System Division) UA team

–Lu Zhao

Program Manager, Active Directory Federation Service

–Aurash Behbahani

Software Design Engineer, Active Directory Federation Service

–Marcelo Mas

Software Design Engineer in Testing, Active Directory Federation Service

Active Directory Rights Management Services

The last (but certainly not least) IDA component in Windows Server 2008 that we'll look at is Active Directory Rights Management Service (AD RMS). As we mentioned at the beginning of this chapter, AD RMS is the follow-up to Windows RMS. Windows RMS is an optional component for the Windows Server 2003 platform that can be used to protect sensitive information stored in documents, in e-mail messages, and on Web sites from unauthorized viewing, modification, or use. AD RMS is designed to work together with RMS-enabled applications such as the Microsoft Office 2007 System and Internet Explorer 7.0, and it also includes a set of core APIs that developers can use to code their own RMS-enabled apps or add RMS functionality to existing apps.

AD RMS works as a client/server system in which an AD RMS server issues rights account certificates that identify trusted entities such as users and services that are permitted to publish rights-protected content. Once a user has been issued such a certificate, the user can assign usage rights and conditions to any content that needs to be protected. For example, the user could assign a condition to an e-mail message that prevents users who read the message from forwarding it to other users. The way this works is that a publishing license is created for the protected content and this license binds the specified usage rights to the piece of content. When the content is distributed, the usage rights are distributed together with it, and users both inside and outside the organization are constrained by the usage rights defined for the content.

Users who receive rights-protected content also require a rights account certificate to access this content. When the recipient of rights-protected content attempts to view or work with this content, the user's RMS-enabled application sends a request to the AD RMS server to request permission to consume this content. The AD RMS licensing service then issues a unique use license that reads, interprets, and applies the usage rights and conditions specified in the publishing licenses. These usage rights and conditions then persist and are automatically applied wherever the content goes. AD RMS relies upon AD DS to verify that a user attempting to consume rights-protected content has the authorization to do so.

AD RMS has been enhanced in several ways in Windows Server 2008 compared with its implementation in Windows Server 2003. These enhancements include an improved installation experience whereby AD RMS can be added as a role using Server Manager; an MMC snap-in for managing AD RMS servers rather than the Web-based interface used in the previous platform; self-enrollment of the AD RMS cluster without the need of Internet connectivity; integration with AD FS to facilitate leveraging existing federated relationships between partners; and the ability to use different AD RMS roles to more effectively delegate the administration of AD RMS servers, policies and settings, rights policy templates, and log files and reports.

Conclusion

Identity and access is key to how businesses communicate in today's connected world. Active Directory in Windows Server 2008 is a significant advance in the evolution of a single, unified, and integrated IDA solution for businesses running Windows-based networks that need to connect to other businesses that are running either Windows or non-Windows networks. Keeping the big picture for IDA in mind helps us to see how all these various improvements to Active Directory work together to provide a powerful platform that can unleash the power of identity for your enterprise.

I know, the Marketing Police are knocking at my door after that last sentence and they want to get me for that one. But whether it sounds like marketing gobbledegook or not, it's true!

Additional Resources

The starting point for finding information about all things IDA on Microsoft platforms is <http://www.microsoft.com/ida/>. Although this link currently redirects you to <http://www.microsoft.com/windowsserver2003/technologies/idm/default.msp>, I have a feeling this will change as Windows Server 2008 approaches RTM.

The Windows Server 2008 main site on Microsoft.com also has a general overview called "Identity and Access in Windows Server Longhorn" that you can read at <http://www.microsoft.com/windowsserver/longhorn/ida-mw.msp>. By the time you read it, there probably will be more details on the site than there are at the time of writing this.

You can also find a developer-side overview of the directory, identity, and access services included in Windows platforms (including Windows Server 2008) on MSDN at <http://msdn2.microsoft.com/en-us/library/aa139675.aspx>.

If you have access to the Windows Server 2008 beta program on Microsoft Connect (<http://connect.microsoft.com>), you can get a lot of detailed information about AD DS, AD CS, AD FS, and so on. First, you'll find the following Step-By-Step guides (and probably others will be there by the time you read this):

- Installing, Configuring, and Troubleshooting OCSP
- Auditing Active Directory Domain Services Changes
- Active Directory Domain Services Backup and Recovery
- Planning, Deploying, and Using a Read-Only Domain Controller
- Restartable Active Directory

- Certificate Settings
- Active Directory Rights Management Services
- Identity Federation with Active Directory Rights Management Services
- Active Directory Domain Services Installation and Removal
- Active Directory Federation Services

Be sure also to turn to Chapter 14, “Additional Resources,” for more sources of information concerning the Windows server core installation option, and also for links to webcasts, whitepapers, blogs, newsgroups, and other sources of information about all aspects of Windows Server 2008.