

JOHN POLICELLI

Active Directory

Domain Services 2008

HOW-TO

Real Solutions for Active Directory 2008 Administrators

SAMS

Active Directory Domain Services 2008 How-To

Copyright © 2009 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

This material may be distributed only subject to the terms and conditions set forth in the Open Publication License, v1.0 or later (the latest version is presently available at <http://www.opencontent.org/openpub/>).

ISBN-13: 978-0-672-33045-2

ISBN-10: 0-672-33045-8

Library of Congress Cataloging-in-Publication Data
Policelli, John.

Active directory 2008 how-to / John Policelli.
p. cm.

ISBN-13: 978-0-672-33045-2

ISBN-10: 0-672-33045-8

1. Directory services (Computer network technology) 2. Microsoft
Windows. I. Title.

TK5105.595.P65 2009

005.7'1376-dc22

2009011935

Printed in the United States of America

First Printing

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Sams Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Bulk Sales

Sams Publishing offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales

1-800-382-3419

corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales

international@pearson.com

Editor-in-Chief

Karen Gettman

Executive Editor

Neil Rowe

Development Editor

Mark Renfrow

Managing Editor

Patrick Kanouse

Project Editor

Mandie Frank

Copy Editor

Megan Wade

Indexer

Ken Johnson

Proofreader

Leslie Joseph

Technical Editor

Todd Meister

Publishing

Coordinator

Cindy Teeters

Designer

Gary Adair

Compositor

Bronkella

Publishing LLC

INTRODUCTION

Overview of This Book

Active Directory has been on the market for roughly a decade now. Prior to Windows Server 2008, the changes in Active Directory functionality had been relatively minuscule in comparison to the changes introduced in Windows Server 2008. Windows Server 2008 is the first Windows Server operating system release to introduce such significant changes to Active Directory functionality since its inception in Windows 2000 Server. Now is likely the most important time for IT professionals to familiarize themselves with the new Active Directory Domain Services (AD DS) in Windows Server 2008.

IT professionals have access to more resources today than ever before. An infinite number of websites, blogs, newsgroups, magazines, and books claim to provide you with the latest and greatest Active Directory information. With the information overload we are experiencing today, it is a task in itself to decipher the profuse amount of information and find exactly what you are looking for.

Look no further! IT professionals can turn to this book first, to get reliable, easy-to-implement solutions they can trust—and use immediately. This completely up-to-date book brings together tested, step-by-step procedures for planning, installing, customizing, and managing AD DS in any production environment. This hands-on how-to guide walks you through performing approximately 200 tasks, with clear and accurate steps and diagrams for each one.

How-To Benefit from This Book

We've designed this book to be easy to read from cover to cover. This book will provide you with the ability to gain a full understanding of Active Directory Domain Services in Windows Sever 2008, while breaking down the subject matter into 13 easy-to-navigate chapters. They include

- ▶ Introduction to Active Directory Domain Services
- ▶ Prepare for Active Directory Domain Services Installation
- ▶ Install and Uninstall Active Directory Domain Services
- ▶ Manage Trusts and Functional Levels
- ▶ Manage Operations Master Roles and Global Catalog Servers
- ▶ Manage Sites and Replication

- ▶ Manage the Active Directory Domain Services Schema
- ▶ Manage Active Directory Domain Services Data
- ▶ Manage Group Policy
- ▶ Manage Password Replication Policies
- ▶ Manage Fine-Grained Password and Account Lockout Policies
- ▶ Manage Active Directory Domain Services Backup and Recovery
- ▶ Manage Active Directory Domain Services Auditing

Within each of these chapters are subheadings that focus on the primary elements of administering that portion of AD DS.

Beneath the subheadings are Scenario/Problem introductions. These serve as mini-starting points for the administrator to consider. At times, the information provided helps you deal with a specific problem you might be facing; however, typically a scenario is described that enables you to determine whether this direction is necessary for your particular organization.

How-To Continue Expanding Your Knowledge

Certainly there are more books, articles, and sites you can and should consider in expanding your knowledge of Windows Server 2008 Active Directory Domain Services, especially because it will no doubt continue to evolve and change as more and more features, fixes, and enhancements are added by Microsoft. How does one stay on top of the flood of information?

Well, several sites are invaluable. They include the following:

- ▶ **The Active Directory Domain Services Microsoft TechNet Library** (<http://technet.microsoft.com/en-ca/library/cc770946.aspx>)—This has to be one of the most valuable online resources for Windows Server 2008 AD DS information. Here you will find getting started guides, the AD DS planning and architecture guide, the AD DS deployment guide, the AD DS operations guide, and the AD DS Installed Help.
- ▶ **What's New in AD DS in Windows Server 2008 Microsoft document** (<http://technet.microsoft.com/en-us/library/cc755093.aspx>)—This document provides a great overview of each of the new AD DS features in Windows Server 2008, as well as links to more granular information on each new feature.
- ▶ **Ask the Directory Services Team Blog** (<http://blogs.technet.com/askds>)—This is Microsoft's official Enterprise Platform Support DS blog.
- ▶ **Discussions in Active Directory** (http://www.microsoft.com/communities/newsgroups/en-us/default.aspx?dg=microsoft.public.windows.server.active_directory)—This is Microsoft's Active Directory newsgroup.

In addition, several blog sites from Active Directory MVPs, Microsoft employees, and Active Directory gurus are worth investigating, including the following:

- ▶ <http://blogs.dirteam.com> (Dirteam.com/ActiveDir.org)
- ▶ <http://www.identityblog.com> (Kim Cameron)
- ▶ <http://blogs.technet.com/ad> (Tim Springston)
- ▶ <http://blog.joeware.net> (Joe Richards)
- ▶ <http://www.gilkirkpatrick.com/Blog> (Gil Kirkpatrick)
- ▶ <http://www.open-a-socket.com> (Tony Murray)
- ▶ <http://briandesmond.com/blog> (Brian Desmond)

These are just a handful of the ones I personally enjoy, although you will easily find many more. Choose the ones you feel are most helpful to you.

Last, but certainly not least, you are welcome to visit my website for free AD DS education: <http://www.policelli.com>. It includes a link to my blog, articles I've written, a variety of publications, and so forth.

CHAPTER 3

Install and Uninstall Active Directory Domain Services

IN THIS CHAPTER:

- ▶ Install a New Windows Server 2008 Forest
- ▶ Install a New Windows Server 2008 Child Domain
- ▶ Install a New Windows Server 2008 Domain Tree
- ▶ Install an Additional Windows Server 2008 Domain Controller
- ▶ Perform a Staged Installation of a Read-Only Domain Controller
- ▶ Install AD DS from Restored Backup Media
- ▶ Remove a Domain Controller from a Domain
- ▶ Forcing the Removal of a Windows Server 2008 Domain Controller
- ▶ Performing Metadata Cleanup
- ▶ Rename a Domain Controller

Active Directory Domain Services (AD DS) was introduced with the release of Windows 2000 Server and has been included in each subsequent release of the server operating system from Microsoft. The majority of companies have at least one AD DS forest deployed. However, some companies continue to deploy new AD DS forests for various reasons.

This chapter describes the steps required to install and uninstall Active Directory Domain Services.

Install a New Windows Server 2008 Forest

Scenario/Problem: In some cases, you will deploy a new Windows Server 2008 Active Directory Domain Service forest instead of adding domain controllers (DCs) to an existing forest. Although the installation of a new Windows Server 2008 AD DS forest does not require any of the preparation steps that were performed in Chapter 2, “Prepare for Active Directory Domain Services Installation,” you still need to perform the installation following specific steps.

Solution: Installing a new Windows Server 2008 forest consists of promoting a Windows Server 2008 server to a domain controller. Thereafter, additional DCs and domains can be added to the new forest. The installation of a new Windows Server 2008 forest can be performed by using the Windows interface, the command line, and an answer file.

Install a New Forest by Using the Windows Interface

To install a new forest by using the Windows interface, perform the following steps using a local account that has membership in the following local group:

► Administrators

1. Log on to the server you want to promote to a domain controller.
2. Click Start and then click Server Manager.
3. In Roles Summary, click Add Roles.
4. On the Before You Begin page, click Next.
5. On the Select Server Roles page, shown in Figure 3.1, click the Active Directory Domain Services check box; then click Next.
6. On the Active Directory Domain Services page, click Next.
7. On the Confirm Installation Selections page, click Install.
8. On the Installation Results page, shown in Figure shown in Figure 3.2, verify that the installation succeeded and then click Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).

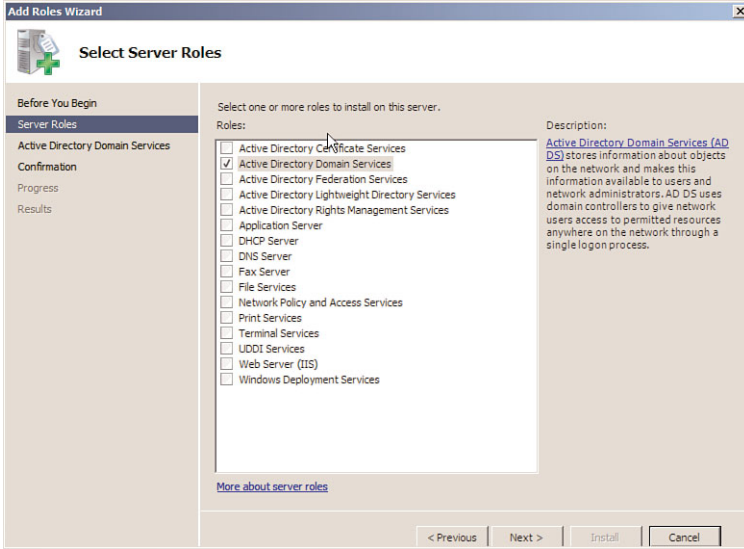


FIGURE 3.1
The Select Server Roles page.

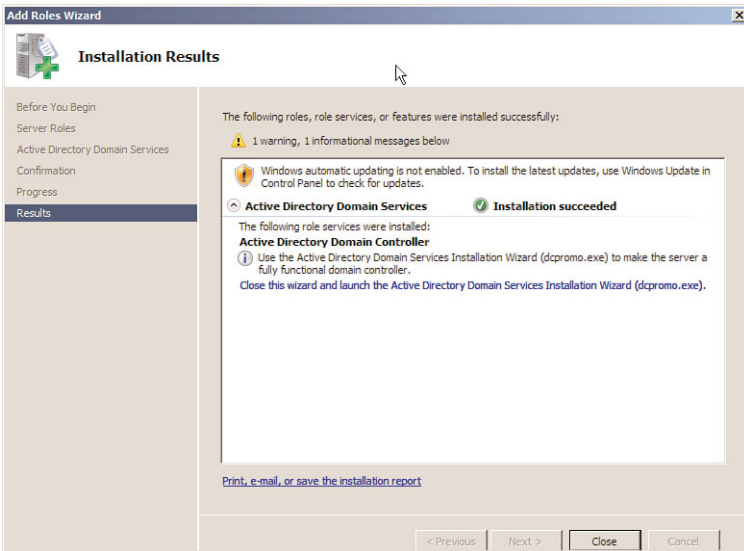


FIGURE 3.2
The Installation Results page.

TIP It is a best practice to assign a static IP address as opposed to a dynamic IP address on a domain controller. If you have not assigned a static IP address, now is the best time to do so. If you proceed with the steps that follow without assigning a static IP address, you will be presented with a warning during the AD DS installation process. You can accept the warning and proceed with the installation if desired.

9. On the Welcome to the Active Directory Domain Services Installation Wizard page, click Next.
10. On the Operating System Compatibility page, click Next.
11. On the Choose a Deployment Configuration page, shown in Figure 3.3, click Create a new domain in a new forest; then click Next.

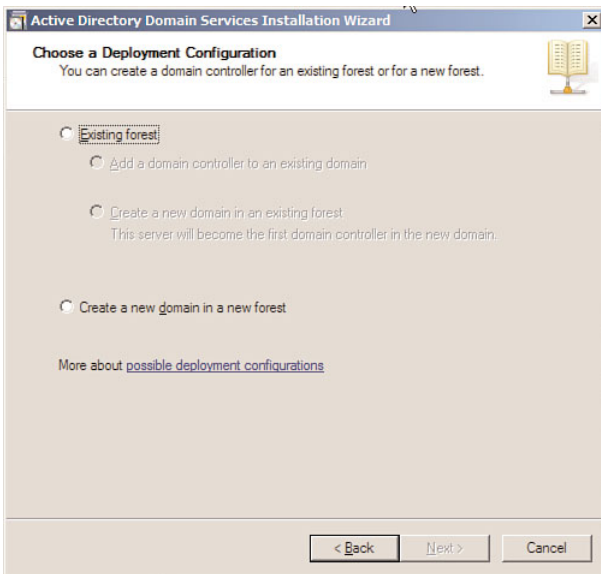


FIGURE 3.3
The Choose a Deployment Configuration page.

12. On the Name the Forest Root Domain page, shown in Figure 3.4, type the fully qualified domain name (FQDN) for the forest root domain and then click Next.
13. On the Set Forest Functional Level page, shown in Figure 3.5, select the forest functional level that meets your requirements and click Next.

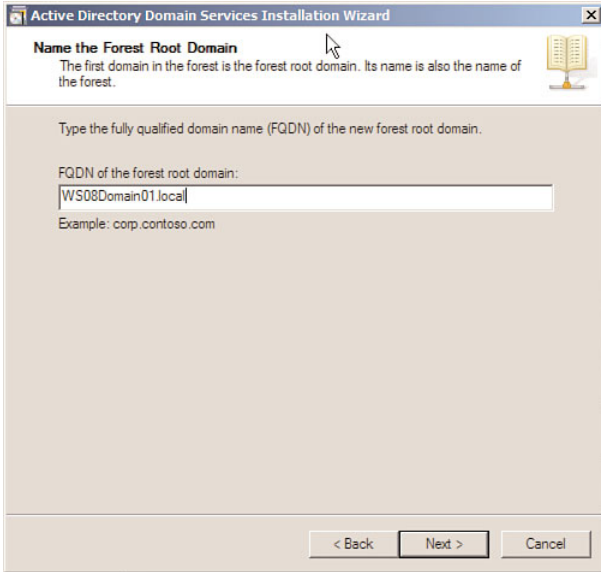


FIGURE 3.4
The Name the Forest Root Domain page.

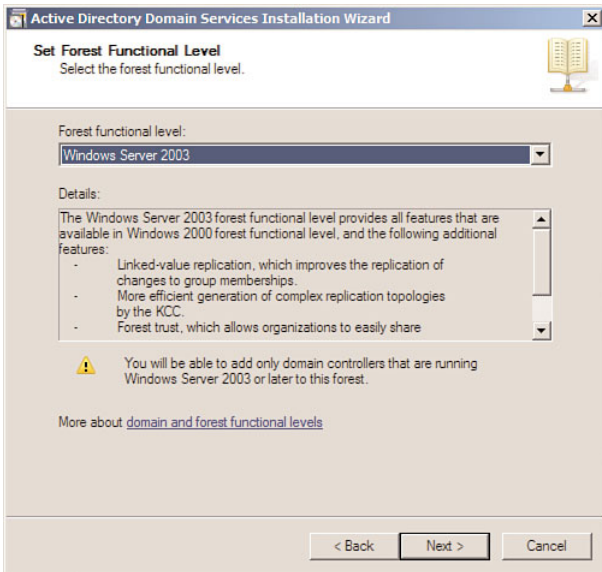


FIGURE 3.5
The Set Forest Functional Level page.

NOTE Active Directory Domain Services functional levels control the available domain or forest advanced features. For example, a number of the new features introduced in Windows Server 2008 require a domain functional level of Windows Server 2008. Functional levels also control the operating systems that you can run on domain controllers. If your domain functional level is set to Windows Server 2008, you cannot have domain controllers that have Windows Server 2003 installed. Lastly, once you set or raise a functional level, you cannot change the functional level to a lower level.

For more information on AD DS functional levels, go to <http://technet.microsoft.com/en-us/library/cc754918.aspx>.

14. If you set a forest functional level other than Windows Server 2008, the Set Domain Functional Level page displays, as shown in Figure 3.6. Select the domain functional level that meets your requirements and click Next.

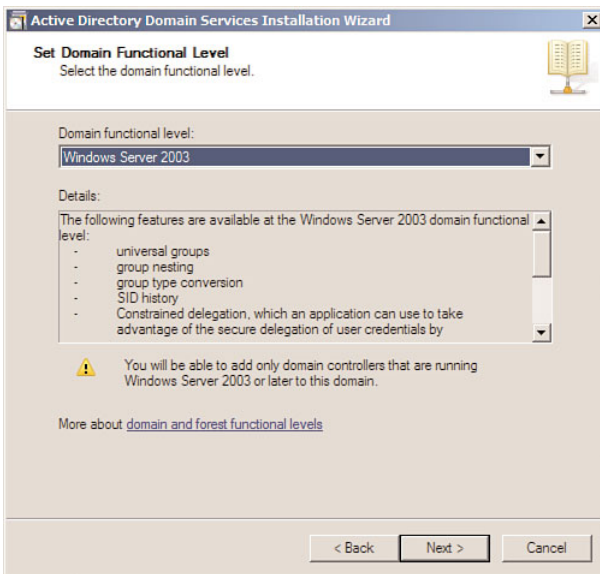


FIGURE 3.6
The Set Domain Functional Level page.

15. On the Additional Domain Controller Options page, shown in Figure 3.7, DNS Server is selected by default, which allows the DNS infrastructure to be created by the installation process. If you plan to use AD-Integrated DNS, click Next. If you plan to use an existing DNS infrastructure and do not want the domain controller to be a DNS server, clear the DNS Server check box and click Next.

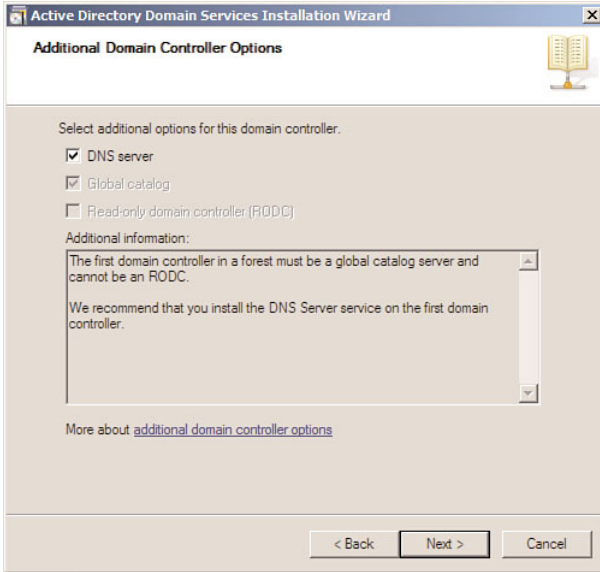


FIGURE 3.7
The Additional Domain Controller Options page.

16. If the wizard cannot create a delegation for the DNS server, it displays a message to indicate that you can create the delegation manually, as shown in Figure 3.8. To continue, click Yes.



FIGURE 3.8
The manual DNS Delegation Message.

17. On the Location for Database, Log Files, and SYSVOL page, shown in Figure 3.9, type the volume and folder locations for the database file, the directory service log files, and the SYSVOL files; then click Next.

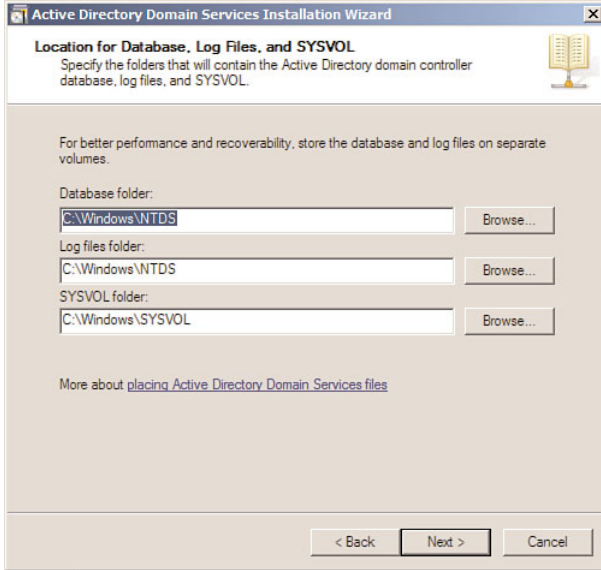


FIGURE 3.9
The Location for Database, Log Files, and SYSVOL page.

18. On the Directory Services Restore Mode Administrator Password page, shown in Figure 3.10, type and confirm the restore mode password and then click Next.

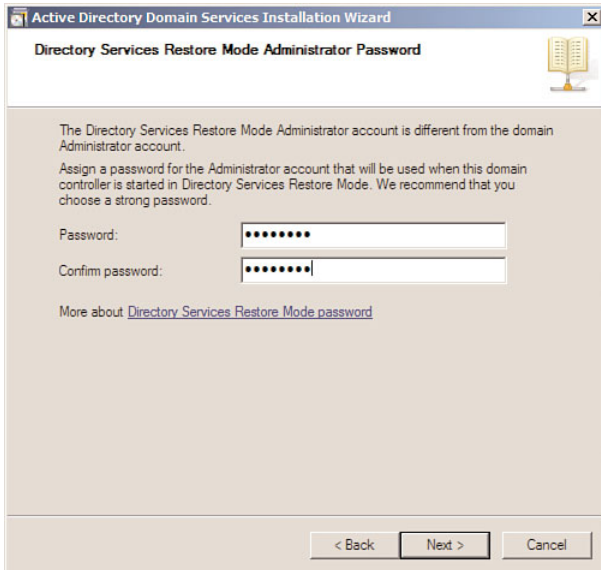


FIGURE 3.10
The Directory Services Restore Mode Administrator Password page.

19. On the Summary page, shown in Figure 3.11, click Next after you review your selections.

TIP You can click the Export button to export the selections you made to an answer file, which can be used later for an unattended installation.

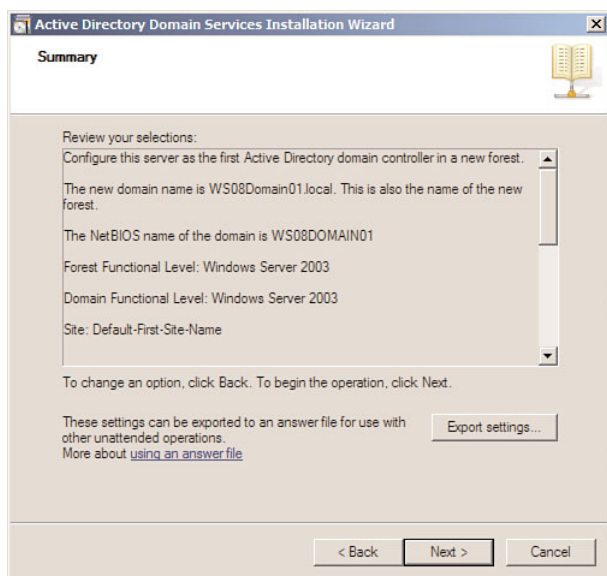


FIGURE 3.11
The Summary page.

The Active Directory Domain Services installation process starts, as shown in Figure 3.12.

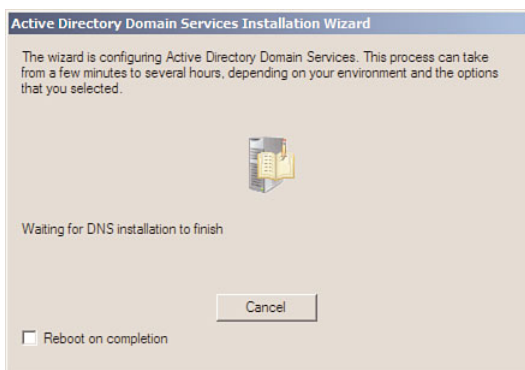


FIGURE 3.12
The Active Directory Domain Services Installation page.

20. After the installation is complete, the Completing the Active Directory Domain Services Installation Wizard page appears, as shown in Figure 3.13. Ensure the installation was successful and click Finish.

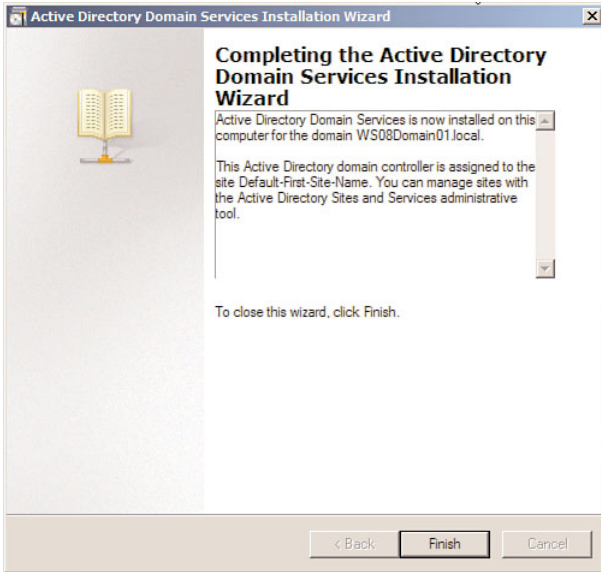


FIGURE 3.13

The Completing the Active Directory Domain Services Installation Wizard page.

21. When prompted to restart, click Restart Now.
22. To validate the installation process, click Start, click Run, type **C:\Windows\Debug**, and click OK.
23. Open the DCPROMO.log file and analyze the results in the file.

Install a New Forest by Using the Command Line

Active Directory Domain Services can also be installed by using the command line. This is particularly useful when installing AD DS on a server that has a Server Core installation of Windows Server 2008.

The installation options when using the command line are the same as those used when installing AD DS using an unattended installation. When installing AD DS by using the command line, you type the installation options and parameters into the command line as opposed to an answer file, which is used for an unattended installation.

Table 3.1 lists the installation parameters used in the steps that follow and the corresponding action of each parameter.

TABLE 3.1 Installing a New Forest by Using the Command Line Installation Parameters

Installation Parameter	Corresponding Action
<code>InstallDns:yes</code>	DNS server will be installed.
<code>dnsOnNetwork:No</code>	DNS server will be installed.
<code>replicaOrNewDomain:domain</code>	A new domain will be created.
<code>newDomain:forest</code>	A new forest will be created.
<code>newDomainDnsName:WS08Domain02.local</code>	FQDN of the new domain.
<code>DomainNetbiosName:WS08Domain02</code>	NetBIOS name of the new domain.
<code>databasePath:"c:\Windows\ntds"</code>	Database path.
<code>logPath:"c:\Windows\ntds"</code>	Log file path.
<code>sysvolpath:"c:\Windows\sysvol"</code>	SYSVOL path.
<code>safeModeAdminPassword:Today01!</code>	DSRM Administrator password.
<code>forestLevel:2</code>	Forest functional level will be set to Windows Server 2003.
<code>domainLevel:2</code>	Domain functional level will be set to Windows Server 2003.
<code>rebootOnCompletion:yes</code>	Server will be rebooted after completion.

TIP For a complete list of installation options and parameters, go to <http://technet.microsoft.com/en-us/library/cc733048.aspx>.

To install a new forest by using the command line, perform the following steps using a local account that has membership in the following local group:

► Administrators

1. Log on to the server you want to promote to a domain controller.
2. Click Start and then click Command Prompt.
3. Type the following into the command prompt window, as shown in Figure 3.14, and then press Enter:

```
dcpromo /unattend /InstallDns:yes /dnsOnNetwork:no  
/replicaOrNewDomain:domain /newDomain:forest  
/newDomainDnsName:WS08Domain02.local  
/DomainNetbiosName:WS08Domain02 /databasePath:"c:\Windows\ntds"  
/logPath:"c:\Windows\ntds" /sysvolpath:"c:\Windows\sysvol"  
/safeModeAdminPassword:Today01! /forestLevel:2 /domainLevel:2  
/rebootOnCompletion:yes
```

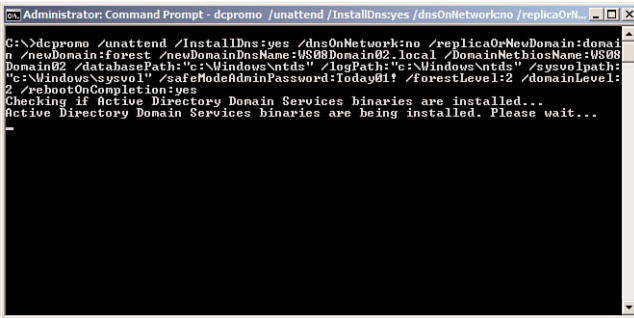



```
Administrator: Command Prompt
C:\>dcpromo /unattend /installDns:yes /dnsOnNetwork:no /replicaOfNewDomain:domain/newDomain:forest /newDomainDnsName:US88Domain02.local /DomainNetbiosName:US88Domain02 /databasePath:"c:\Windows\ntds" /logPath:"c:\Windows\ntds" /sysvolpath:"c:\Windows\sysvol" /safeModeAdminPassword:Today01! /forestLevel:2 /domainLevel:2 /rebootOnCompletion:yes_
```

FIGURE 3.14

Installing a new forest using the command line.

The dcpromo process begins by determining whether the AD DS binaries are installed. If the binaries are not installed, dcpromo installs them, as shown in Figure 3.15.



```
Administrator: Command Prompt - dcpromo /unattend /installDns:yes /dnsOnNetwork:no /replicaOfNewDomain:domain/newDomain:forest /newDomainDnsName:US88Domain02.local /DomainNetbiosName:US88Domain02 /databasePath:"c:\Windows\ntds" /logPath:"c:\Windows\ntds" /sysvolpath:"c:\Windows\sysvol" /safeModeAdminPassword:Today01! /forestLevel:2 /domainLevel:2 /rebootOnCompletion:yes
Checking if Active Directory Domain Services binaries are installed...
Active Directory Domain Services binaries are being installed. Please wait...
_
```

FIGURE 3.15

Installing AD DS services binaries.

4. After the AD DS binaries have been installed, a summary of the installation options is presented in the command prompt window, as shown in Figure 3.16. Then the AD DS installation process begins.
5. The status of the AD DS installing is updated in the command prompt window, as shown in Figure 3.17.

```
Administrator: Command Prompt - dcpromo /unattend /InstallDns:yes /dnsOnNetwork:no /replicaOrti...
The following actions will be performed:
Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is WS08Domain02.local. This is also the name of the new forest.

The NetBIOS name of the domain is WS08Domain02

Forest Functional Level: Windows Server 2003
Domain Functional Level: Windows Server 2003
Site: Default-First-Site-Name

Additional Options:
  Read-only domain controller: No
  Global catalog: Yes
  DNS Server: Yes

Create DNS Delegation: No

Database folder: c:\Windows\ntds
Log file folder: c:\Windows\ntds
SYSVOL folder: c:\Windows\sysvol

The DNS Server service will be installed on this computer.
The DNS Server service will be configured on this computer.
This computer will be configured to use this DNS server as its preferred DNS server.

The password of the new domain Administrator will be the same as the password of the local Administrator of this computer.

Starting...
```

FIGURE 3.16
Installing AD DS.

```
Administrator: Command Prompt - dcpromo /unattend /InstallDns:yes /dnsOnNetwork:no /replicaOrti...
Creating directory partition: CN=Configuration,DC=WS08Domain02,DC=local; 0 objects remaining
Creating directory partition: DC=WS08Domain02,DC=local; 0 objects remaining
Creating Active Directory Domain Services objects on the local Active Directory Domain Controller
Creating new domain users, groups, and computer objects
Configuring service kdc

Setting the LSA policy information
Setting the computer's DNS computer name root to WS08Domain02.local

Setting security on the domain controller and Directory Service files and registry keys

Securing machine\software\microsoft\windows
```

FIGURE 3.17
The installation's progress.

6. When the installation process is complete, the server reboots automatically if the `/rebootOnCompletion` option was used in the command line. If the `/rebootOnCompletion` option was not used in the command line, you are prompted to restart the server.
7. To validate the installation process, click Start, click Run, type `C:\Windows\Debug`, and click OK.
8. Open the DCPROMO.log file and analyze the results in the file.

Install a New Forest by Using an Answer File

Active Directory Domain Services can also be installed using an answer file. This is useful when installing AD DS on a server that has a Server Core installation of Windows Server 2008.

Table 3.2 lists the installation parameters used in the steps that follow and the corresponding action of each parameter.

TABLE 3.2 Installing a New Forest by Using Answer File Installation Parameters

Installation Parameter	Corresponding Action
InstallDNS=yes	DNS server will be installed.
NewDomain=forest	A new forest will be created.
NewDomainDNSName=WS08Domain03.local	FQDN of the new domain.
DomainNetBiosName=WS08Domain03	NetBIOS name of the new domain.
ReplicaOrNewDomain=domain	A new domain will be created.
ForestLevel=3	Forest functional level will be set to Windows Server 2008.
DomainLevel=3	Domain functional level will be set to Windows Server 2008.
DatabasePath="c:\Windows\ntds"	Database path.
LogPath="c:\Windows\ntds"	Log file path.
RebootOnCompletion=yes	Server will be rebooted after completion.
SYSVOLPath=c:\Windows\sysvol	SYSVOL path.
SafeModeAdminPassword=Today01!	DSRM Administrator password.

TIP For a complete list of installation options and parameters, go to <http://technet.microsoft.com/en-us/library/cc733048.aspx>.

In order to install a new forest by using an answer file, perform the following steps using a local account that has membership in the following local group:

- ▶ Administrators
1. Log on to the server you want to promote to a domain controller.
 2. Click Start, click Run, type **notepad**, and click OK.
 3. On the first line, type **[DCINSTALL]**, and then press ENTER.

4. Type the following entries, one entry on each line, as shown in Figure 3.18:

```

InstallDNS=yes
NewDomain=forest
NewDomainDNSName=WS08Domain03.local
DomainNetBiosName=WS08Domain03
ReplicaOrNewDomain=domain
ForestLevel=3
DomainLevel=3
DatabasePath="c:\Windows\ntds"
LogPath="c:\Windows\ntds"
RebootOnCompletion=yes
SYSVOLPath="c:\Windows\sysvol"
SafeModeAdminPassword=Today01!

```

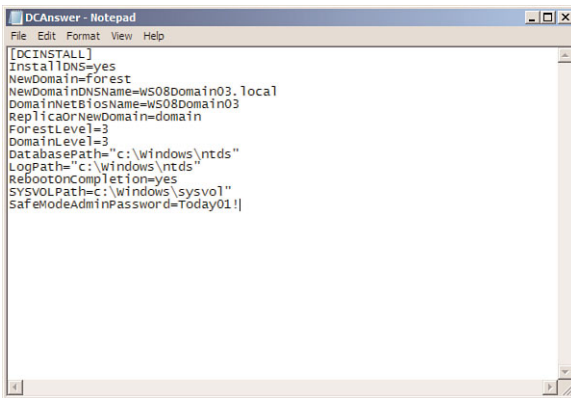


FIGURE 3.18
The answer file.

5. Save the answer file as `C:\DCAnswer.txt`.
6. Click Start and then click Command Prompt.
7. Type the following into the command prompt window, as shown in Figure 3.19, and then press Enter:

```
dcpromo /unattend:"C:\DCAnswer.txt"
```

The `dcpromo` process begins by determining whether the AD DS binaries are installed. If the binaries are not installed, `dcpromo` installs them.

8. After the AD DS binaries have been installed, a summary of the installation options is presented in the command prompt window; then the AD DS installation process begins. The status of the AD DS installing is updated in the command prompt window.

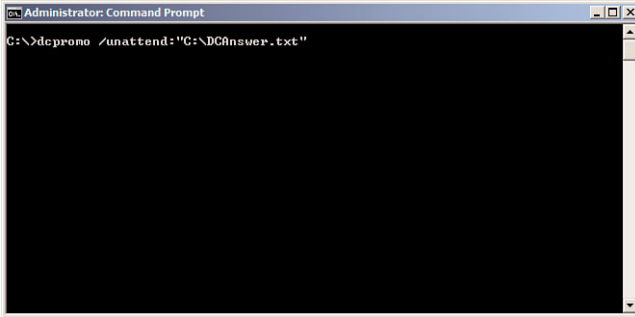


FIGURE 3.19
Installing a new forest by using an answer file.

9. When the installation process is complete, the server reboots automatically if the `/rebootOnCompletion` option was used in the answer file. If the `/rebootOnCompletion` was not used in the answer file, you are prompted to restart the server.
10. To validate the installation process, click Start, click Run, type **C:\Windows\Debug**, and click OK.
11. Open the `DCPROMO.log` file and analyze the results in the file.

Install a New Windows Server 2008 Child Domain

Scenario/Problem: You require additional domains within your AD DS forest. If the new domain is to share a contiguous namespace with one or more domains, you need to create a new child domain.

Solution: Installing a new Windows Server 2008 child domain consists of selecting the option to create a new child domain during the promotion of a domain controller. The installation of a new Windows Server 2008 child domain can be performed using the Windows interface, the command line, and an answer file.

TIP If you are installing a new Windows Server 2008 child domain into an existing Windows Server 2008 forest, you do not have to prepare the forest before you begin the installation. However, if you are installing a new Windows Server 2008 child domain into an existing Windows 2000 Server or Windows Server 2003 forest, you must first prepare the forest by performing the steps in Chapter 2.

Install a Child Domain by Using the Windows Interface

To install a child domain by using the Windows interface, perform the following steps using an AD DS account that has membership in the following AD DS group:

- ▶ Enterprise Administrators
1. Log on to the server you want to promote to a domain controller.
 2. Click Start and then click Server Manager.
 3. In Roles Summary, click Add Roles.
 4. On the Before You Begin page, click Next.
 5. On the Select Server Roles page, click the Active Directory Domain Services check box; then click Next.
 6. On the Active Directory Domain Services page, click Next.
 7. On the Confirm Installation Selections page, shown in Figure 3.20, click Install.

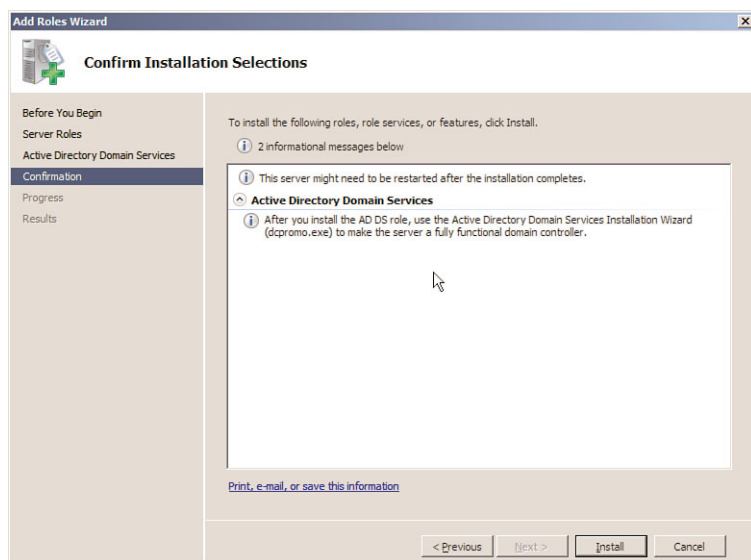


FIGURE 3.20

The Confirm Installation Selections page.

8. On the Installation Results page, shown in Figure 3.21, verify that the installation succeeded and then click Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).

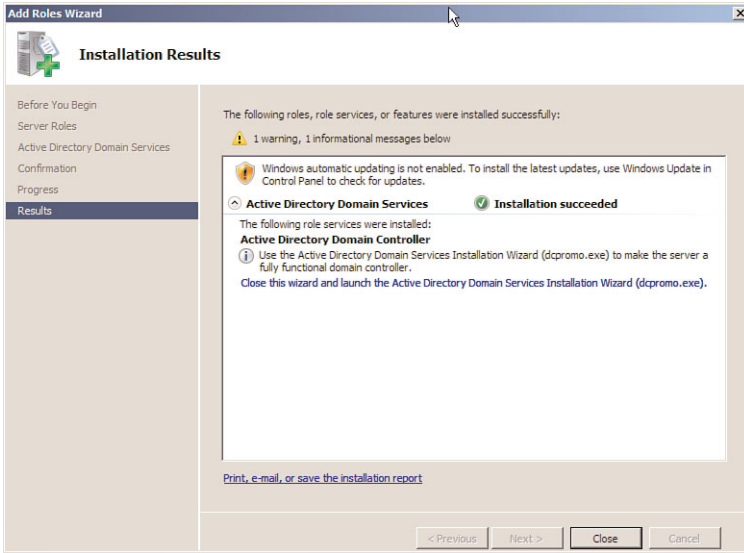


FIGURE 3.21
The Installation Results page.

9. On the Welcome to the Active Directory Domain Services Installation Wizard page, shown in Figure 3.22, click Next.



FIGURE 3.22
The Welcome to the Active Directory Domain Services Installation Wizard page.

10. On the Operating System Compatibility page, shown in Figure 3.23, click Next.

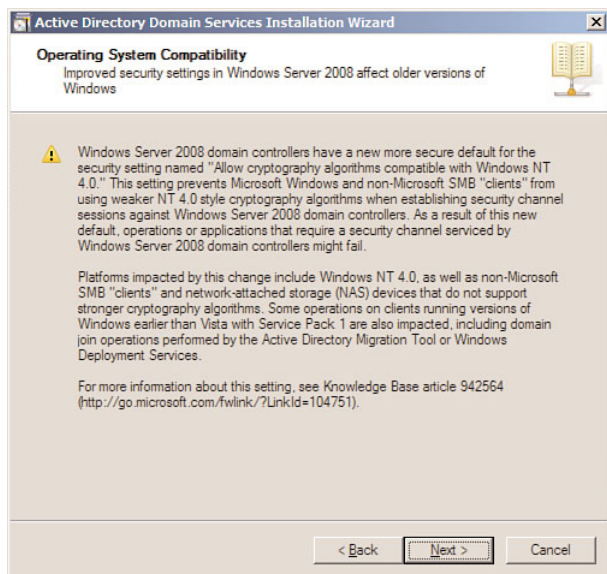


FIGURE 3.23

The Operating System Compatibility page.

11. On the Choose a Deployment Configuration page, select Existing forest, select Create a new domain in an existing forest, and click Next.
12. On the Network Credentials page, shown in Figure 3.24, type the DNS name of the domain you want to join. Under Specify the account credentials to use to perform the installation, click Alternate Credentials; then click Set. On the Windows Security dialog box, enter the username and password for an account that has the permission to add the domain to the forest, and then click OK. Click Next to proceed.
13. On the Name the New Domain page, shown in Figure 3.25, type the FQDN of the parent domain and the Single-label DNS name of the child domain. Then click Next.

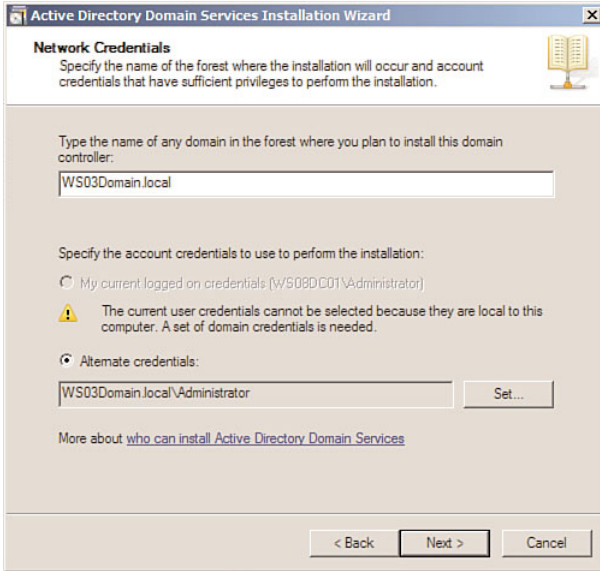


FIGURE 3.24
The Network Credentials page.

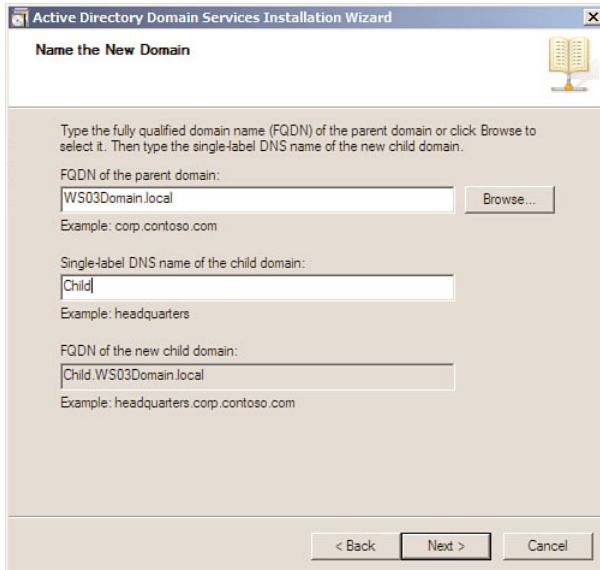


FIGURE 3.25
The Name the New Domain page.

14. On the Set Domain Functional Level page, Select the domain functional level that meets your requirements and click Next.
15. On the Select a Site page, shown in Figure 3.26, select the site to which you want the domain controller to belong and click Next.

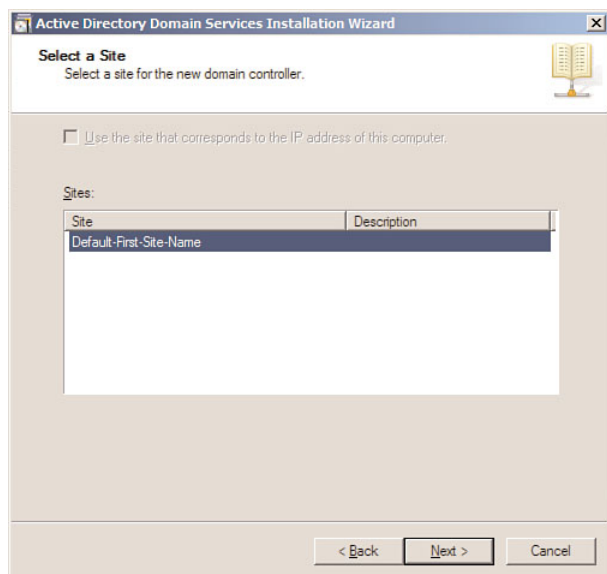


FIGURE 3.26
The Select a Site page.

16. On the Additional Domain Controller Options page, select the desired additional options for the domain controller and click Next.
17. On the Location for Database, Log Files, and SYSVOL page, type the volume and folder locations for the database file, the directory service log files, and the SYSVOL files; then click Next.
18. On the Directory Services Restore Mode Administrator Password page, type and confirm the restore mode password and then click Next.
19. On the Summary page, click Next after you review your selections.

The Active Directory Domain Services installation process starts, as shown in Figure 3.27.

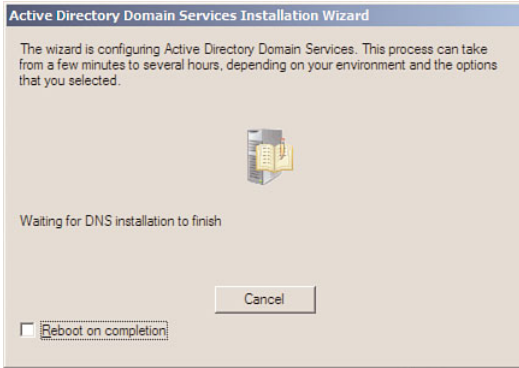


FIGURE 3.27

The Active Directory Domain Services Installation Wizard screen.

20. After the installation is complete, the Completing the Active Directory Domain Services Installation Wizard page appears. Ensure the installation was successful and click Finish.
21. When prompted to restart, click Restart Now.
22. To validate the installation process, click Start, click Run, type **C:\Windows\Debug**, and click OK.
23. Open the DCPROMO.log file and analyze the results in the file.

Install a Child Domain by Using the Command Line

Table 3.3 lists the installation parameters used in the steps that follow and the corresponding action of each parameter.

TABLE 3.3 Installing a Child Domain by the Command Line Installation Parameters

Installation Parameter	Corresponding Action
/InstallDns:yes	DNS server will be installed.
/ParentDomainDNSName:WS03Domain.local	Name of the parent domain to which this domain will be added.
/replicaOrNewDomain:domain	A new domain will be created.
/newDomain:child	The new domain will be a child domain.
/newDomainDnsName:child02.WS03Domain.local	FQDN of the new child domain.
/childName:child02	Name of the new child domain.
/DomainNetbiosName:child02	NetBIOS name of the new child domain.
/databasePath:"c:\Windows\ntds"	Database path.

TABLE 3.3 Installing a Child Domain by the Command Line Installation

Parameters (continued)

Installation Parameter	Corresponding Action
/logPath:"c:\Windows\ntds"	Log file path.
/sysvolpath:"c:\Windows\sysvol"	SYVOL path.
/safeModeAdminPassword:Today01!	DSRM Administrator password.
/forestLevel:2	Forest functional level will be set to Windows Server 2003.
/domainLevel:2	Domain functional level will be set to Windows Server 2003.
/rebootOnCompletion:no	Server will not be rebooted after completion.
/userName:WS03Domain\Administrator	The username that will be used to promote the server to a domain controller.
/userDomain:WS03Domain	The domain of the user account that will be used to promote the server to a domain controller.
/password:Today01!	The password of the user that will be used to promote the server to a domain controller.

TIP For a complete list of installation options and parameters, go to <http://technet.microsoft.com/en-us/library/cc733048.aspx>.

To install a child domain by using the command line, perform the following steps using an AD DS account that has membership in the following AD DS group:

- ▶ Enterprise Administrators

1. Log on to the server you want to promote to a domain controller.
2. Click Start and then click Command Prompt.
3. Type the following into the command prompt window and then press Enter:

```
dcpromo /unattend /InstallDns:yes
/ParentDomainDNSName:WS03Domain.local
/replicaOrNewDomain:domain /newDomain:child
/newDomainDnsName:child02.WS03Domain.local /childName:child02
/DomainNetbiosName:child02 /databasePath:"c:\Windows\ntds"
/logPath:"c:\Windows\ntds" /sysvolpath:"c:\Windows\sysvol"
/safeModeAdminPassword:Today01! /forestLevel:2 /domainLevel:2
/rebootOnCompletion:no /userName:WS03Domain\Administrator
/userDomain:WS03Domain /password:Today01!
```

The dcpromo process begins by determining whether the AD DS binaries are installed. If the binaries are not installed, dcpromo installs them.

4. After the AD DS binaries have been installed, a summary of the installation options is presented in the command prompt window; then the AD DS installation process begins.
5. The status of the AD DS installing is updated in the command prompt window.
6. When the installation process is complete, the server reboots automatically if the /rebootOnCompletion option was used in the command line. If the /rebootOnCompletion was not used in the command line, you are prompted to restart the server, as shown in Figure 3.28.

```

Administrator Command Prompt
Securing Kerberos Policy
The attempted domain controller operation has completed

Configuring the DNS Server service on this computer...
Active Directory Domain Services is now installed on this computer for the domain child02.ws03domain.local.

This Active Directory domain controller is assigned to the site Default-First-Site-Name. You can manage sites with the Active Directory Sites and Services administrative tool.

Windows Server 2008 domain controllers have a new more secure default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0." This setting prevents Microsoft Windows and non-Microsoft SMB "clients" from using weaker NT 4.0 style cryptography algorithms when establishing security channel sessions against Windows Server 2008 domain controllers. As a result of this new default, operations or applications that require a security channel serviced by Windows Server 2008 domain controllers might fail.

Platforms impacted by this change include Windows NT 4.0, as well as non-Microsoft SMB "clients" and network-attached storage (NAS) devices that do not support stronger cryptography algorithms. Some operations on clients running versions of Windows earlier than Vista with Service Pack 1 are also impacted, including domain join operations performed by the Active Directory Migration Tool or Windows Deployment Services.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

Some errors occurred during the operation. Consult the event log for more information.

You must restart this computer to complete the operation.

C:\>

```

FIGURE 3.28

Installation complete.

The installation is complete.

7. To validate the installation process, click Start, click Run, type **C:\Windows\Debug**, and click OK.
8. Open the DCPROMO.log file and analyze the results in the file.

Install a Child Domain by Using an Answer File

Table 3.4 lists the installation parameters used in the steps that follow and the corresponding action of each parameter.

TABLE 3.4 Installing a Child Domain by Using Answer File Installation Parameters

Installation Parameter	Corresponding Action
ParentDomainDNSName=WS03Domain.local	Name of parent domain to which this domain will be added.
UserName=WS03Domain\Administrator	The username that will be used to promote the server to a domain controller.
UserDomain:WS03Domain	The domain of the user account that will be used to promote the server to a domain controller.
Password=Today01!	The password of the user that will be used to promote the server to a domain controller.
NewDomain=child	The new domain will be a child domain.
ChildName=Child03	The new domain will be a child domain.
DomainNetBiosName=Child03	NetBIOS name of the new child domain.
ReplicaOrNewDomain=domain	Forest functional level will be set to Windows Server 2003.
DomainLevel=2	Domain functional level will be set to Windows Server 2003.
DatabasePath="c:\Windows\ntds"	Database path.
LogPath="c:\Windows\ntds"	Log file path.
SYSVOLPath="c:\Windows\sysvol"	SYSVOL path.
InstallDNS=yes	DNS server will be installed.
SafeModeAdminPassword=Today01!	DSRM Administrator password.
RebootOnCompletion=no	Server will not be rebooted after completion.

TIP For a complete list of installation options and parameters, go to <http://technet.microsoft.com/en-us/library/cc733048.aspx>.

To install a child domain by using an answer file, perform the following steps using an AD DS account that has membership in the following AD DS group:

- ▶ Enterprise Administrators
1. Log on to the server you want to promote to a domain controller.
 2. Click Start, click Run, type **notepad**, and click OK.
 3. On the first line, type **[DCINSTALL]**; then press ENTER.

4. Type the following entries, one entry on each line, as shown in Figure 3.29:

```

ParentDomainDNSName=WS03Domain.local
UserName=WS03Domain\Administrator
UserDomain=WS03Domain
Password=Today01!
NewDomain=child
ChildName=Child03
DomainNetBiosName=Child03
ReplicaOrNewDomain=domain
DomainLevel=2
DatabasePath="c:\Windows\ntds"
LogPath="c:\Windows\ntds"
SYSVOLPath="c:\Windows\sysvol"
InstallDNS=yes
SafeModeAdminPassword=Today01!
RebootOnCompletion=no

```

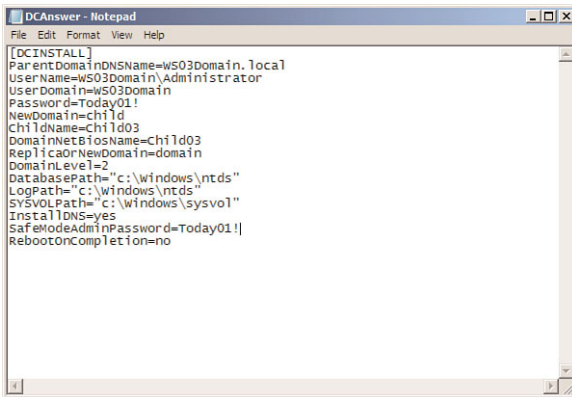


FIGURE 3.29
The answer file.

5. Save the answer file as C:\DCAnswer.txt.
6. Click Start and then click Command Prompt.
7. Type the following into the command prompt window, as shown in Figure 3.30, and then press Enter:

```
dcpromo /unattend:"C:\DCAnswer.txt"
```

The `dcpromo` process begins by determining whether the AD DS binaries are installed. If the binaries are not installed, `dcpromo` installs them.

8. After the AD DS binaries have been installed, a summary of the installation options is presented in the command prompt window; then the AD DS installation process begins. The status of the AD DS installing is updated in the command prompt window, as shown in Figure 3.31.

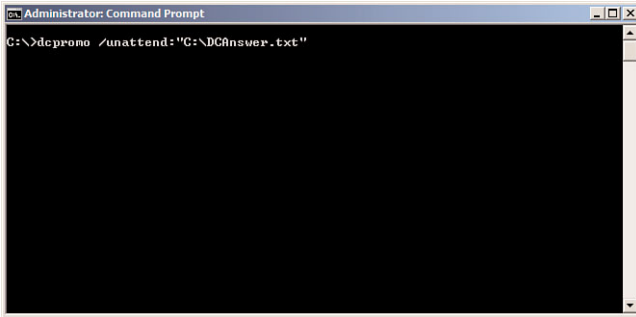


FIGURE 3.30
Installing a new child domain using an answer file.

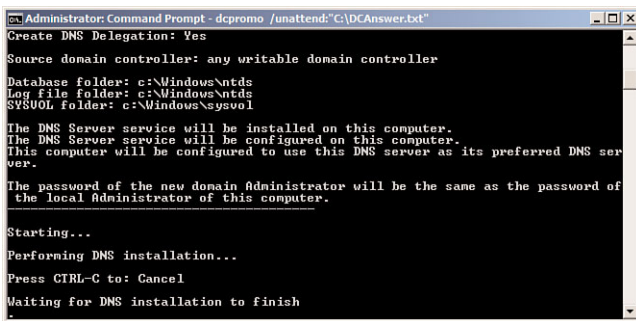


FIGURE 3.31
The status of installing AD DS.

9. When the installation process is complete, the server reboots automatically if the `/rebootOnCompletion` option was used in the answer file. If the `/rebootOnCompletion` was not used in the answer file, you are prompted to restart the server.
10. To validate the installation process, click Start, click Run, type in **C:\Windows\Debug**, and click OK.
11. Open the DCPROMO.log file and analyze the results in the file.

Install a New Windows Server 2008 Domain Tree

Scenario/Problem: When you create a new domain in a forest and the domain DNS namespace is not related to the other domains in the forest, you need to create a new domain tree.

Solution: Installing a new Windows Server 2008 domain tree consists of selecting the option to create a new domain tree during the promotion of a DC. The installation of a new Windows Server 2008 domain tree can be performed using the Windows interface, the command line, and an answer file.

TIP If you are installing a new Windows Server 2008 domain tree in an existing Windows Server 2008 forest, you do not have to prepare the forest before you begin the installation. However, if you are installing a new Windows Server 2008 domain tree in an existing Windows 2000 Server or Windows Server 2003 forest, you must first prepare the forest by performing the steps in Chapter 2.

Install a Domain Tree by Using the Windows Interface

To install a domain tree by using the Windows interface, perform the following steps using an AD DS account that has membership in the following AD DS group:

- ▶ Enterprise Administrators

1. Log on to the server you want to promote to a domain controller.
2. Click Start, click Run, type **dcprmo**, and click OK.
3. The AD DS server role is installed, as shown in Figure 3.32.

TIP The AD DS server role can be installed by using the `dcprmo` command.

4. On the Welcome to the Active Directory Domain Services Installation Wizard page, select the Use Advanced Mode Installation option and click Next.
5. On the Operating System Compatibility page, click Next.
6. On the Choose a Deployment Configuration page, select Existing forest, select Create a new domain in an existing forest, select the Create a new domain tree root instead of a new child domain check box, and then click Next.
7. On the Network Credentials page, type the DNS name of the domain you want to join. Under Specify the account credentials to use to perform the installation, click Alternate credentials, and then click Set. On the Windows Security dialog box, enter the username and password for an account that has the permission to add the domain to the forest; then click OK. Click Next to proceed.

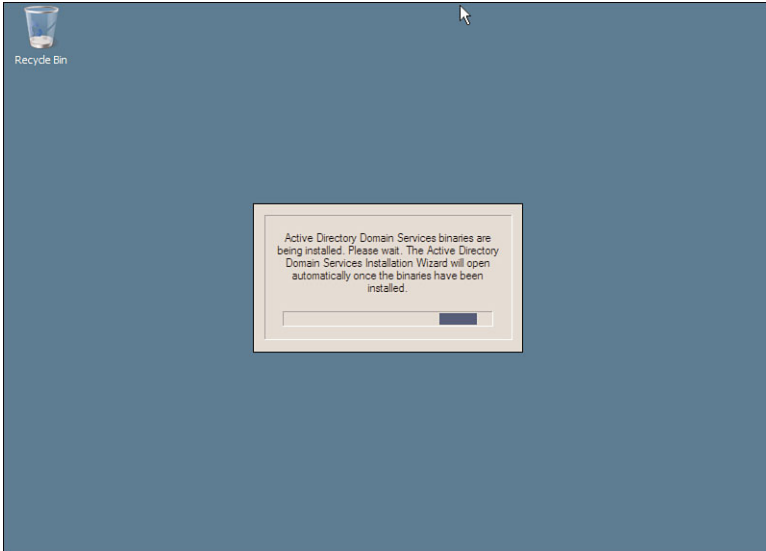


FIGURE 3.32
Installing AD DS server role using dcpromo.

8. On the Name the New Domain Tree Root page, shown in Figure 3.33, type the FQDN of the new domain tree and click Next.

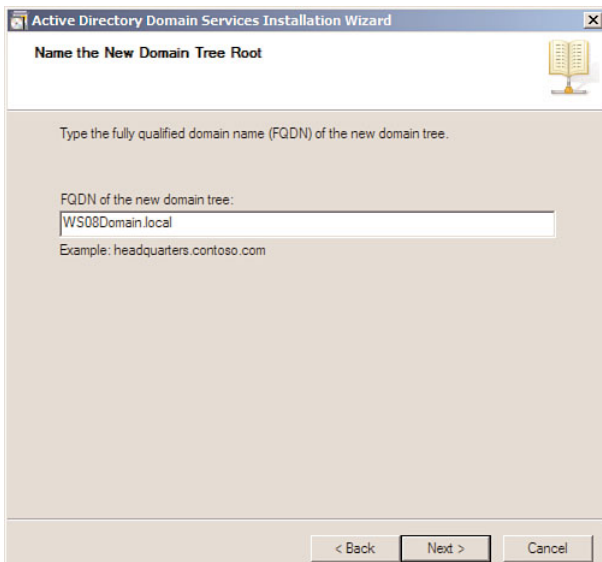


FIGURE 3.33
The Name the New Domain Tree Root page.

9. On the Domain NetBIOS Name page, shown in Figure 3.34, enter the NetBIOS name for the new domain tree and click Next.

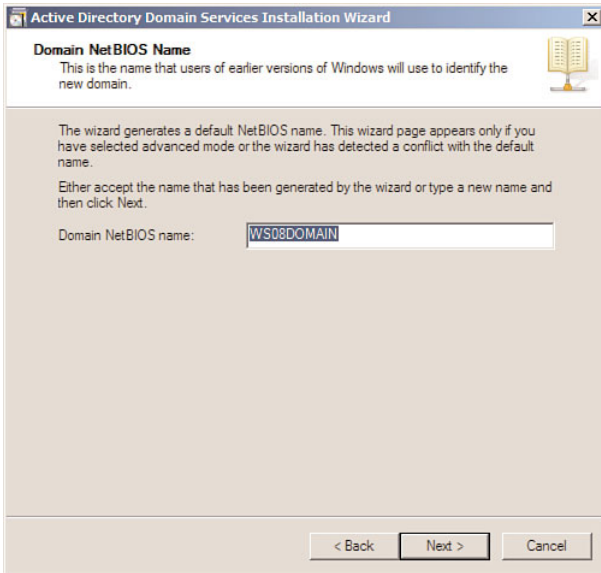


FIGURE 3.34
The Domain NetBIOS Name page.

10. On the Set Domain Functional Level page, select the domain functional level that meets your requirements and click Next.
11. On the Select a Site page, select the site to which you want the domain controller to belong and click Next.
12. On the Additional Domain Controller Options page, select the desired additional options, such as DNS server and/or Global catalog, for the domain controller and click Next.
13. On the Location for Database, Log Files, and SYSVOL page, type the volume and folder locations for the database file, the directory service log files, and the SYSVOL files; then click Next.
14. On the Directory Services Restore Mode Administrator Password page, type and confirm the restore mode password. Then click Next.
15. On the Summary page, click Next after you review your selections.

The Active Directory Domain Services installation process starts, as shown in Figure 3.35.

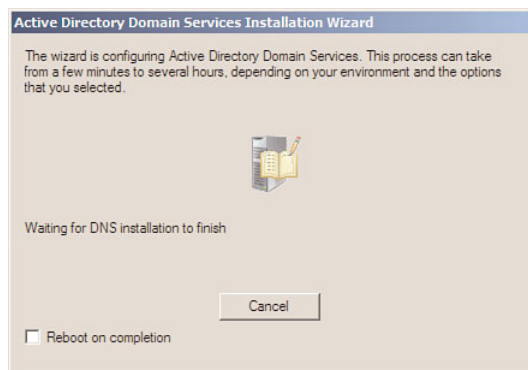


FIGURE 3.35
The Active Directory Domain
Services Installation Wizard page.

16. After the installation is complete, the Completing the Active Directory Domain Services Installation Wizard page appears. Ensure the installation was successful and click Finish.
17. When prompted to restart, click Restart Now.
18. To validate the installation process, click Start, click Run, type **C:\Windows\Debug**, and click OK.
19. Open the DCPROMO.log file and analyze the results in the file.

Install a Domain Tree by Using the Command Line

Table 3.5 lists the installation parameters used in the steps that follow and the corresponding action of each parameter.

TABLE 3.5 **Installing a Domain Tree by Using the Command Line Installation Parameters**

Installation Parameter	Corresponding Action
/InstallDns:yes	DNS server will be installed.
/ParentDomainDNSName:WS03Domain.local	Name of the forest root domain to which this domain tree will be added.
/replicaOrNewDomain:domain	A new domain will be created.
/newDomain:tree	The new domain will be a new domain tree.
/newDomainDnsName:WS08DomainB.local	FQDN of the new domain tree.
/DomainNetbiosName:WS08DomainB	NetBIOS name of the new domain tree.
/databasePath:"c:\Windows\ntds"	Database path.
/logPath:"c:\Windows\ntds"	Log file path.
/sysvolpath:"c:\Windows\sysvol"	SYSVOL path.
/safeModeAdminPassword:Today01!	DSRM Administrator password.

continues

TABLE 3.5 Installing a Domain Tree by Using the Command Line Installation Parameters (continued)

Installation Parameter	Corresponding Action
/forestLevel:2	Forest functional level will be set to Windows Server 2003.
/domainLevel:2	Domain functional level will be set to Windows Server 2003.
/rebootOnCompletion:no	Server will not be rebooted after completion.
/userName:WS03Domain\Administrator	The username that will be used to promote the server to a domain controller.
/userDomain:WS03Domain	The domain of the user account that will be used to promote the server to a domain controller.
/password:Today01!	The password of the user that will be used to promote the server to a domain controller.

TIP For a complete list of installation options and parameters, go to <http://technet.microsoft.com/en-us/library/cc733048.aspx>.

To install child domain tree by using the command line, perform the following steps using an AD DS account that has membership in the following AD DS group:

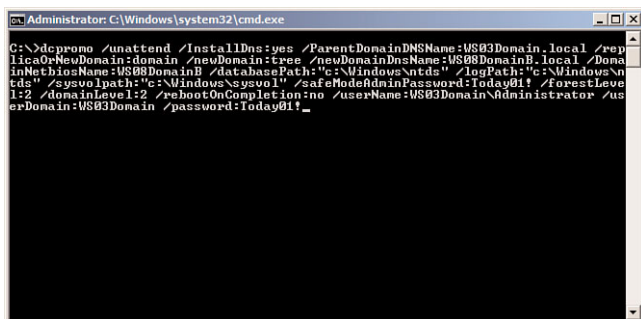
► Enterprise Administrators

1. Log on to the server you want to promote to a domain controller.
2. Click Start and then click Command Prompt.
3. Type the following into the command prompt window, as shown in Figure 3.36, and then press Enter:

```

dcpromo /unattend /InstallDns:yes
/ParentDomainDNSName:WS03Domain.local
/replicaOrNewDomain:domain /newDomain:tree
/newDomainDnsName:WS08DomainB.local /DomainNetbiosName:WS08DomainB
/databasePath:"c:\Windows\ntds" /logPath:"c:\Windows\ntds"
/sysvolpath:"c:\Windows\sysvol" /safeModeAdminPassword:Today01!
/forestLevel:2 /domainLevel:2 /rebootOnCompletion:no
/userName:WS03Domain\Administrator /userDomain:WS03Domain
/password:Today01!

```



```

Administrator: C:\Windows\system32\cmd.exe
C:\>dcpromo /unattend /installDns=yes /ParentDomainDNSName:WS03Domain.local /replicaOrNewDomain=domain /newDomain=tree /newDomainDNSName:WS08DomainB.local /DomainNetbiosName:WS08DomainB /databasePath:"c:\Windows\system32" /logPath:"c:\Windows\system32" /sysprepPath:"c:\Windows\system32" /safeModeAdminPassword:Today01! /forestLevel:2 /domainLevel:2 /rebootOnCompletion:no /userName:WS03Domain\Administrator /userDomain:WS03Domain /password:Today01!

```

FIGURE 3.36

Installing a new domain tree using the command line.

The dcpromo process begins by determining whether the AD DS binaries are installed. If the binaries are not installed, dcpromo installs them.

4. After the AD DS binaries have been installed, a summary of the installation options is presented in the command prompt window; then the AD DS installation process begins.
5. The status of the AD DS installing is updated in the command prompt window.
6. When the installation process is complete, the server reboots automatically if the /rebootOnCompletion option was used in the command line. If the /rebootOnCompletion was not used in the command line, you are prompted to restart the server.
7. To validate the installation process, click Start, click Run, type **C:\Windows\Debug**, and click OK.
8. Open the DCPROMO.log file and analyze the results in the file.

Install a Domain Tree by Using an Answer File

Table 3.6 lists the installation parameters used in the steps that follow and the corresponding action of each parameter.

TABLE 3.6 Installing a Domain Tree by Using Answer File Installation Parameters

Installation Parameter	Corresponding Action
installDns=yes	DNS server will be installed.
ParentDomainDNSName=WS03Domain.local	Name of the forest root domain to which this domain tree will be added.
replicaOrNewDomain=domain	A new domain will be created.
newDomain=tree	The new domain will be a new domain tree.

continues

TABLE 3.6 Installing a Domain Tree by Using Answer File Installation

Parameters (continued)

Installation Parameter	Corresponding Action
newDomainDnsName=WS08DomainC.local	FQDN of new domain tree.
DomainNetbiosName=WS08DomainC	NetBIOS name of the new domain tree.
databasePath="c:\Windows\ntds"	Database path.
logPath="c:\Windows\ntds"	Log file path.
Sysvolpath="c:\Windows\sysvol"	SYSVOL path.
safeModeAdminPassword=Today01!	DSRM Administrator password.
forestLevel=2	Forest functional level will be set to Windows Server 2003.
domainLevel=2	Domain functional level will be set to Windows Server 2003.
rebootOnCompletion=no	Server will not be rebooted after completion.
userName=WS03Domain\Administrator	The username that will be used to promote the server to a domain controller.
userDomain=WS03Domain	The domain of the user account that will be used to promote the server to a domain controller.
Password=Today01!	The password of the user that will be used to promote the server to a domain controller.

TIP For a complete list of installation options and parameters, go to <http://technet.microsoft.com/en-us/library/cc733048.aspx>.

To install child domain tree by using an answer file, perform the following steps using an AD DS account that has membership in the following AD DS group:

► Enterprise Administrators

1. Log on to the server you want to promote to a domain controller.
2. Click Start, click Run, type **notepad**, and click OK.
3. On the first line, type **[DCINSTALL]**; then press ENTER.
4. Type the following entries, one entry on each line:

```
InstallDns=yes
ParentDomainDNSName=WS03Domain.local
replicaOrNewDomain=domain
newDomain=tree
newDomainDnsName=WS08DomainC.local
```

```
DomainNetbiosName=WS08DomainC
databasePath="c:\Windows\ntds"
logPath="c:\Windows\ntds"
sysvolpath="c:\Windows\sysvol"
safeModeAdminPassword=Today01!
forestLevel=2
domainLevel=2
rebootOnCompletion=no
userName=WS03Domain\Administrator
userDomain=WS03Domain
password=Today01!
```

5. Save the answer file as C:\DCAnswer.txt.
6. Click Start and then click Command Prompt.
7. Type the following into the command prompt window, as shown in Figure 3.37, and then press ENTER:

```
dcpromo /unattend:"C:\DCAnswer.txt"
```

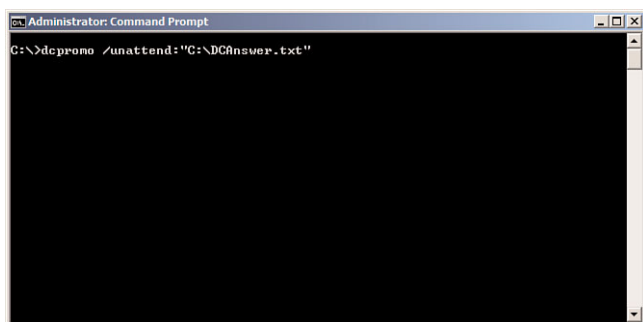


FIGURE 3.37

Installing a domain tree using an answer file.

The `dcpromo` process begins by determining whether the AD DS binaries are installed. If the binaries are not installed, `dcpromo` installs them.

8. After the AD DS binaries have been installed, a summary of the installation options is presented in the command prompt window. Then the AD DS installation process begins. The status of the AD DS installing is updated in the command prompt window.
9. When the installation process is complete, the server reboots automatically if the `/rebootOnCompletion` option was used in the answer file. If the `/rebootOnCompletion` was not used in the answer file, you are prompted to restart the server.

10. To validate the installation process, click Start, click Run, type **C:\Windows\Debug**, and click OK.
11. Open the DCPROMO.log file and analyze the results in the file.

Install an Additional Windows Server 2008 Domain Controller

Scenario/Problem: To provide adequate fault tolerance and optimize authentication, you require a minimum of two DCs.

Solution: Installing an additional Windows Server 2008 DC consists of promoting a member server to a DC in an existing domain. The installation of an additional Windows Server 2008 DC can be performed using the Windows interface, the command line, and an answer file.

TIP If you are installing an additional Windows Server 2008 DC in an existing Windows Server 2008 forest, you do not have to prepare the forest before you begin the installation. However, if you are installing an additional Windows Server 2008 DC in an existing Windows 2000 Server or Windows Server 2003 forest, you must first prepare the forest; then you must prepare the domain in which the DC will reside. This can be done by performing the steps in Chapter 2.

Install an Additional Domain Controller by Using the Windows Interface

To install an additional DC by using the Windows interface, perform the following steps using an AD DS account that has membership in the following AD DS group:

- ▶ Domain Admins for the domain for which you want to add a writable domain controller.
1. Log on to the server you want to promote to a domain controller.
 2. Click Start, Run, type in **dcpromo**, and click OK.
 3. The dcpromo process begins by determining whether the AD DS binaries are installed. If the binaries are not installed, dcpromo installs them.
 4. After the dcpromo process installs the Active Directory Domain Services server role, the Welcome to the Active Directory Domain Services Installation Wizard page appears. Click Next.
 5. On the Operating System Compatibility page, click Next.

6. On the Choose a Deployment Configuration page, select Existing forest, select Add a domain controller to an existing forest, and click Next.
7. On the Network Credentials page, enter the DNS name of the domain to which you want to add the domain controller. Under Specify the account credentials to use to perform the installation, click Alternate credentials, and then click Set. On the Windows Security dialog box, enter the username and password for an account that has the permission to add the domain to the forest, and then click OK. Click Next to proceed.
8. On the Select a Domain page, shown in Figure 3.38, select the domain to which you want to add the domain controller and click Next.

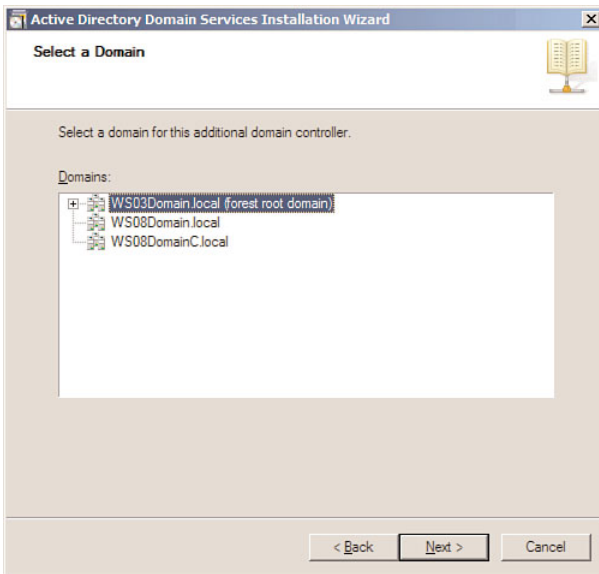


FIGURE 3.38

The Select a Domain page.

9. On the Select a Site page, select the site to which you want the domain controller to belong and click Next.
10. On the Additional Domain Controller Options page, select the desired additional options, such as DNS server and/or Global catalog, for the domain controller and click Next.
11. On the Location for Database, Log Files, and SYSVOL page, type the volume and folder locations for the database file, the directory service log files, and the SYSVOL files; then click Next.
12. On the Directory Services Restore Mode Administrator Password page, type and confirm the restore mode password. Then click Next.

13. On the Summary page, click Next after you review your selections.

The Active Directory Domain Services installation process starts.

14. After the installation is complete, the Completing the Active Directory Domain Services Installation Wizard page appears. Ensure the installation was successful and click Finish.
15. When prompted to restart, click Restart Now.
16. To validate the installation process, click Start, click Run, type **C:\Windows\Debug**, and click OK.
17. Open the DCPROMO.log file and analyze the results in the file.

Install an Additional Domain Controller by Using the Command Line

Table 3.7 lists the installation parameters used in the steps that follow and the corresponding action of each parameter.

TABLE 3.7 Installing an Additional DC by Using the Command Line Installation Parameters

Installation Parameter	Corresponding Action
InstallDns:yes	DNS server will be installed.
confirmGC:yes	Specifies the domain controller is a global catalog server.
replicaOrNewDomain:replica	An additional domain controller will be added to the domain.
replicaDomainDNSName:WS03Domain.local	The DNS name of the domain that the domain controller will be added to.
databasePath:"c:\windows\ntds"	Database path.
logPath:"c:\windows\ntds"	Log file path.
sysvolpath:"c:\windows\sysvol"	SYSVOL path.
safeModeAdminPassword:Today01!	DSRM Administrator password.
rebootOnCompletion:no	Server will not be rebooted after completion.
userName:WS03Domain\Administrator	The username that will be used to promote the server to a domain controller.
userDomain:WS03Domain	The domain of the user account that will be used to promote the server to a domain controller.
password:Today01!	The password of the user that will be used to promote the server to a domain controller.

TIP For a complete list of installation options and parameters, go to <http://technet.microsoft.com/en-us/library/cc733048.aspx>.

To install an additional DC by using the command line, perform the following using an AD DS account that has membership in the following AD DS group:

- ▶ Domain Admins for the domain for which you want to add a writable domain controller.
1. Log on to the server you want to promote to a domain controller.
 2. Click Start and then click Command Prompt.
 3. Type the following into the command prompt window, as shown in Figure 3.39, and then press ENTER:

```
dcpromo /unattend /InstallDns:yes /confirmGC:yes
/replicaOrNewDomain:replica /replicaDomainDNSName:WS03Domain.local
/databasePath:"c:\windows\ntds" /logPath:"c:\windows\ntds"
/sysvolpath:"c:\windows\sysvol" /safeModeAdminPassword:Today01!
/rebootOnCompletion:yes
```

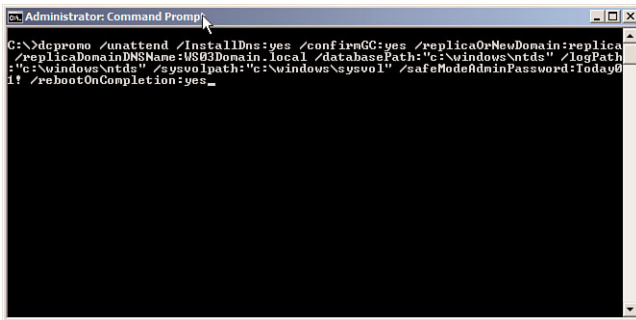


FIGURE 3.39
Installing an additional DC using the command line.

The dcpromo process begins by determining whether the AD DS binaries are installed. If the binaries are not installed, dcpromo installs them.

4. After the AD DS binaries have been installed, a summary of the installation options is presented in the command prompt window; then the AD DS installation process begins.
5. The status of the AD DS installing is updated in the command prompt window.
6. When the installation process is complete, the server reboots automatically if the /rebootOnCompletion option was used in the command line. If the /rebootOnCompletion was not used in the command line, you are prompted to restart the server.

7. To validate the installation process, click Start, click Run, type **C:\Windows\Debug**, and click OK.
8. Open the DCPROMO.log file and analyze the results in the file.

Install an Additional Domain Controller by Using an Answer File

Table 3.8 lists the installation parameters used in the steps that follow and the corresponding action of each parameter.

TABLE 3.8 Installing an Additional DC by Using Answer File Installation Parameters

Installation Parameter	Corresponding Action
InstallDns=yes	DNS server will be installed.
confirmGC=yes	Specifies the domain controller is a global catalog server.
replicaOrNewDomain=replica	An additional domain controller will be added to the domain.
replicaDomainDNSName=WS03Domain.local	The DNS name of the domain to which the domain controller will be added.
databasePath="c:\windows\ntds"	Database path.
logPath="c:\windows\ntds"	Log file path.
sysvolpath="c:\windows\sysvol"	SYSVOL path.
safeModeAdminPassword=Today01!	DSRM Administrator password.
rebootOnCompletion=no	Server will not be rebooted after completion.
userName=WS03Domain\Administrator	The username that will be used to promote the server to a domain controller.
userDomain=WS03Domain	The domain of the user account that will be used to promote the server to a domain controller.
password=Today01!	The password of the user that will be used to promote the server to a domain controller.

TIP For a complete list of installation options and parameters, go to <http://technet.microsoft.com/en-us/library/cc733048.aspx>.

To install an additional DC by using an answer file, perform the following using an AD DS account that has membership in the following AD DS group:

- ▶ Domain Admins for the domain for which you want to add a writable domain controller.

1. Log on to the server you want to promote to a domain controller.
2. Click Start, click Run, type **notepad**, and click OK.
3. On the first line, type **[DCINSTALL]** and then press ENTER.
4. Type the following entries, one entry on each line, as shown in Figure 3.40:

```
InstallDns=yes
confirmGC=yes
replicaOrNewDomain=replica
replicaDomainDNSName=WS03Domain.local
databasePath="c:\windows\ntds"
logPath="c:\windows\ntds"
sysvolpath="c:\windows\sysvol"
safeModeAdminPassword=Today01!
rebootOnCompletion=no
UserName=WS03Domain\Administrator
UserDomain=WS03Domain
Password=Today01!
```

5. Save the answer file as C:\DCAnswer.txt.
6. Click Start and then click Command Prompt.
7. Type the following into the command prompt window, as shown in Figure 3.40, and then press ENTER:

```
dcpromo /unattend:"C:\DCAnswer.txt"
```

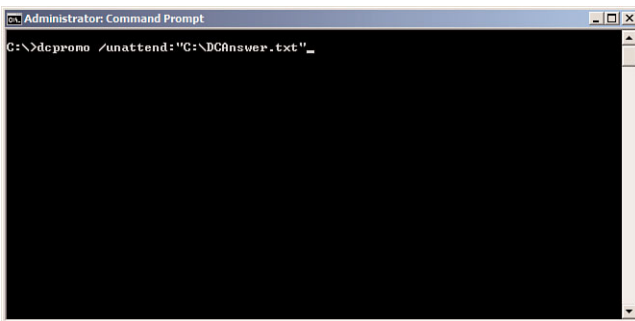


FIGURE 3.40
Installing an additional DC by using an answer file.

The `dcpromo` process begins by determining whether the AD DS binaries are installed. If the binaries are not installed, `dcpromo` installs them.

8. After the AD DS binaries have been installed, a summary of the installation options is presented in the command prompt window; then the AD DS installation process begins. The status of the AD DS installing is updated in the command prompt window.

9. When the installation process is complete, the server reboots automatically if the `/rebootOnCompletion` option was used in the answer file. If the `/rebootOnCompletion` was not used in the answer file, you are prompted to restart the server.
10. To validate the installation process, click Start, click Run, type `C:\Windows\Debug`, and click OK.
11. Open the `DCPROMO.log` file and analyze the results in the file.

Perform a Staged Installation of a Read-Only Domain Controller

Scenario/Problem: You need to deploy a Read-only domain controllers (RODC) in a branch office. You plan to delegate the installation of AD DS on the RODCs to someone physically located in the branch office.

Solution: A staged installation of an RODC consists of two stages. The first stage of the installation creates an account for the RODC in AD DS. The second stage of the installation attaches the server to the account that was created in the first stage. The first stage requires elevated permissions in AD DS. However, the second stage can be performed by someone you delegate the ability to attach the server to the account.

Stage 1: Create an RODC Account in AD DS

To create an RODC account in AD DS, perform the following steps using an AD DS account that has membership in the following AD DS group:

- ▶ Domain Admins for the domain for which you want to add a RODC.
1. Click Start, click Administrative Tools, and then click Active Directory Users and Computers.
 2. Right-click the Domain Controllers Organizational Unit (OU) and select Pre-create Read-only Domain Controller account, as shown in Figure 3.41.
 3. On the Welcome to the Active Directory Domain Services page, shown in Figure 3.42, click Next.

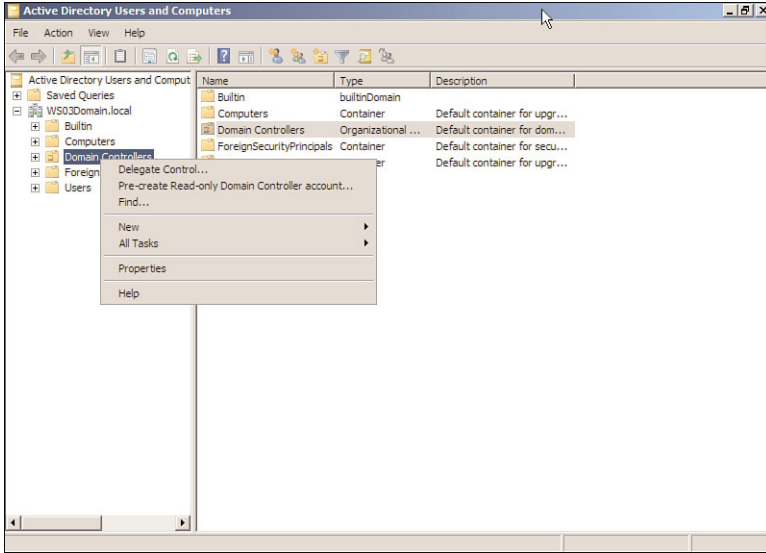


FIGURE 3.41
Selecting Pre-create Read-only Domain Controller account.



FIGURE 3.42
The Welcome to the Active Directory Domain Services page.

4. On the Operating System Compatibility page, click Next.
5. On the Network Credentials page, under Specify the account credentials to use to perform the installation, click My current logged on credentials or click Alternate credentials. If you select Alternate credentials, click Set and in the Windows Security dialog box, provide the user name and password for an account that can install the additional DC. When you are finished providing credentials, click Next.
6. On the Specify the Computer Name page, shown in Figure 3.43, enter the name of the server that will be the RODC; then click Next.

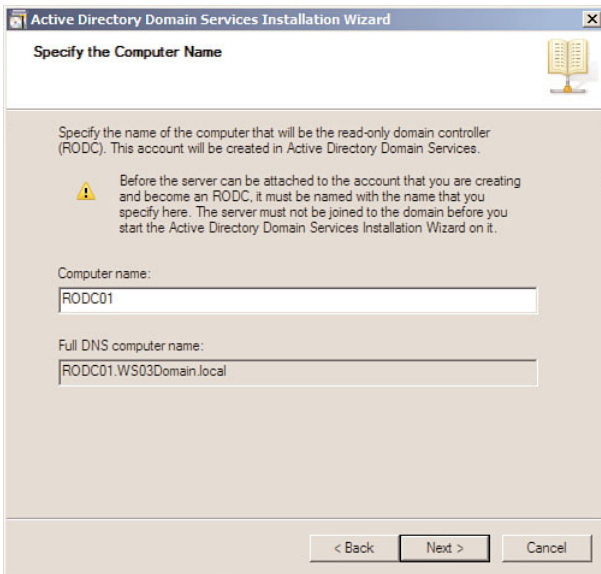


FIGURE 3.43

The Specify the Computer Name page.

7. On the Select a Site page, select the site to which you want the domain controller to belong and click Next.
8. On the Additional Domain Controller Options page, select the desired additional options, such as DNS server and/or Global catalog, for the domain controller and click Next.
9. On the Delegation of RODC Installation and Administration page, shown in Figure 3.44, enter the group or user that can attach the server to the RODC account and click Next.

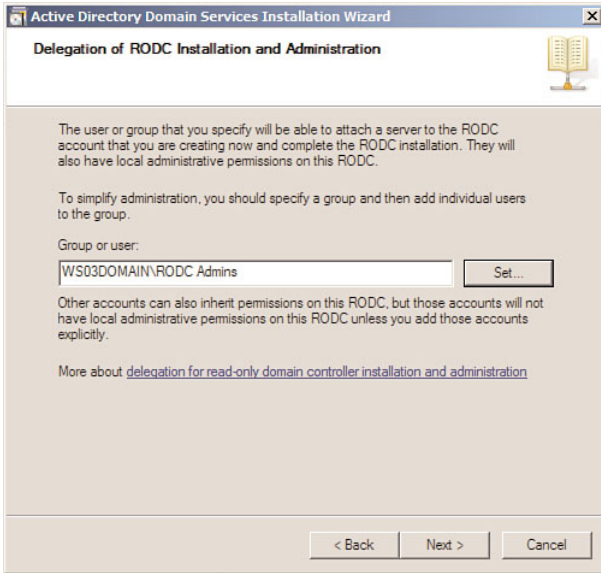


FIGURE 3.44
The Delegation of RODC Installation and Administration page.

10. On the Summary page, click Next.
11. On the Completing the Active Directory Domain Services Installation Wizard page, click Finish.

Stage 2: Attach Server to RODC Account

To attach a server to an RODC account, perform the following steps using an AD DS account that has been delegated the permission to attach the server to the RODC account in stage 1, outlined previously, and with membership in the following local group:

- ▶ Administrators
 1. Log on to the server you want to attach to the RODC account using an account that has been delegated the permission to attach the server to the RODC account in stage 1.
 2. Click Start, click Command Prompt.
 3. In the Command Prompt window, type **dcpromo /UseExistingAccount:Attach** and press ENTER.

The dcpromo process begins by determining whether the AD DS binaries are installed. If the binaries are not installed, dcpromo installs them.

4. On the Welcome to the Active Directory Domain Services Installation Wizard page, click Next.
5. On the Network Credentials page, click Next.
6. On the Select Domain Controller Account page, confirm that the wizard has found an existing RODC account that matches the name of the server; then click Next.
7. On the Location for Database, Log Files, and SYSVOL page, type or browse to the volume and folder locations for the database file, the directory service log files, and the system volume (SYSVOL) files. Then click Next.
8. On the Directory Services Restore Mode Administrator Password page, type and confirm the restore mode password and click Next.
9. On the Summary page, click Next.
10. On the Completing the Active Directory Domain Services Installation Wizard page, click Finish.
11. To validate the installation process, click Start, click Run, type **C:\Windows\Debug**, and click OK.
12. Open the DCPROMO.log file and analyze the results in the file.

Install AD DS from Restored Backup Media

Scenario/Problem: You need to minimize network traffic during the installation of Active Directory Domain Services.

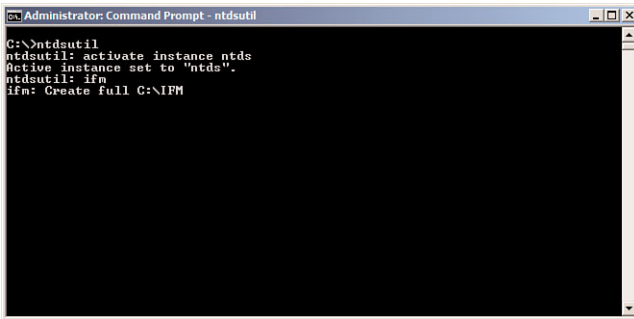
Solution: Install AD DS from restored backup media.

Create Installation Media

To create AD DS installation media, perform the following steps using an account that has the permissions to log on to a DC interactively and be able to make a backup.

1. Log on to the domain controller you will use to create the media.
2. Click Start, and click Command Prompt.
3. In the command prompt window, type **ntdsutil** and press ENTER.
4. At the **ntdsutil** prompt, type **activate instance ntds** and press ENTER.
5. At the **ntdsutil** prompt, type **ifm** and press ENTER.

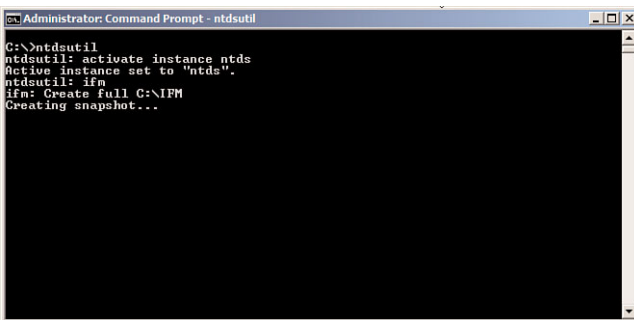
- At the `ifm:` prompt, shown in Figure 3.45, type the command for the type of installation media that you want to create; then press ENTER. To create the media for an RODC, type **Create rodc C:\Folder**, where `C:\Folder` is the path to store the media. To create the media for a full (writable), type **Create full C:\Folder**, where `C:\Folder` is the path to store the media. Press ENTER when complete.



```
Administrator: Command Prompt - ntdsutil
C:\>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: ifm
ifm: Create full C:\IFM
```

FIGURE 3.45
IFM prompt.

- `ntdsutil` creates the installation media, as shown in Figure 3.46.



```
Administrator: Command Prompt - ntdsutil
C:\>ntdsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: ifm
ifm: Create Full C:\IFM
Creating snapshot...
```

FIGURE 3.46
Create ifm installation media.

- When the installation media has been created successfully, you are returned to the `ifm:` prompt, as shown in Figure 3.47.

```

Administrator: Command Prompt - nidsutil
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: ifm
ifm: Create full C:\IFM
Creating snapshot...
Snapshot set {63ab0718-ff32-4df8-896f-573193fc672b} generated successfully.
Snapshot {da36d121-5371-40fb-a0d7-a4b145196dd2} mounted as C:\$SNAP_200808251540_UOLJHECS\
UOLJHECS\
Snapshot {da36d121-5371-40fb-a0d7-a4b145196dd2} is already mounted.
Initiating DEFRAGMENTATION mode...
Source Database: C:\$SNAP_200808251540_UOLJHECS\Windows\NTDS\ntds.dit
Target Database: C:\IFM\Active Directory\ntds.dit

Defragmentation Status (% complete)

  0   10  20  30  40  50  60  70  80  90 100
  |---|---|---|---|---|---|---|---|---|---|
  .....

Copying registry files...
Copying C:\IFM\registry\SYSTEM
Copying C:\IFM\registry\SECURITY
Snapshot {da36d121-5371-40fb-a0d7-a4b145196dd2} unmounted.
IFM media created successfully in C:\IFM
ifm: =

```

FIGURE 3.47

The IFM created successfully.

9. Type **Q** to exit the ifm: prompt.
10. Type **Q** to exit ntdsutl.
11. Close the command prompt window.

Install AD DS from Media

To install AD DS from media, perform the following steps using an account that has the permissions to log on to a DC interactively and be able to make a backup.

1. Log on to the domain controller you will install AD DS on.
2. Click Start, click Run, type **dcpromo**, and click OK.
3. The dcpromo process begins by determining whether the AD DS binaries are installed. If the binaries are not installed, dcpromo installs them.
4. On the Welcome to the Active Directory Domain Services Installation Wizard page, select Use advanced mode installation and click Next.
5. On the Operating System Compatibility page, click Next.
6. On the Choose a Deployment Configuration page, select Existing forest, select Add a domain controller to an existing domain, and click Next.
7. On the Network Credentials page, type the DNS name of the domain you want to join. Under Specify the account credentials to use to perform the installation, click Alternate credentials, and then click Set. On the Windows Security dialog box, enter the user name and password for an account that has the permission to add the domain to the forest; then click OK. Click Next to proceed.
8. On the Select a Domain page, select the domain to which you want to add the domain controller and click Next.

9. On the Select a Site page, select the site to which you want the domain controller to belong and click Next.
10. On the Additional Domain Controller Options page, select the desired additional options for the domain controller and click Next.
11. On the Install from Media page, shown in Figure 3.48, select Replicate data from media at the following location, type the location of the installation media that was previously created, and click Next.

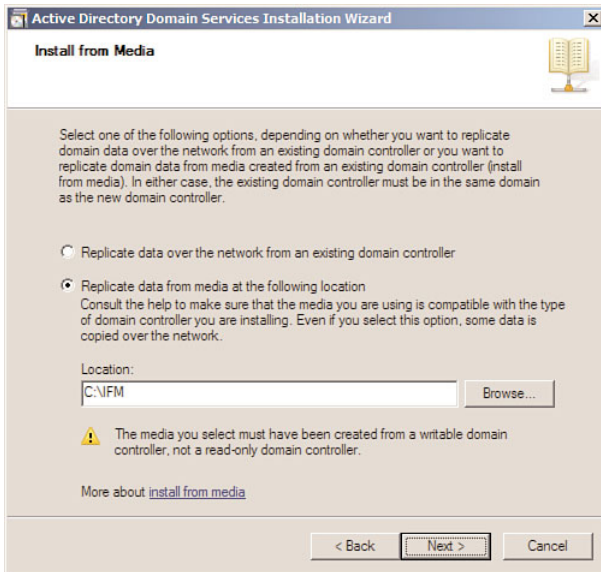


FIGURE 3.48
The Install from Media page.

12. On the Source Domain Controller page, shown in Figure 3.49, select a source domain controller for the installation partner or select Let the wizard choose an appropriate domain controller; then click Next.
13. On the Location for Database, Log Files, and SYSVOL page, type the volume and folder locations for the database file, the directory service log files, and the SYSVOL files; then click Next.
14. On the Directory Services Restore Mode Administrator Password page, type and confirm the restore mode password and click Next.
15. On the Summary page, click Next after you review your selections.
The Active Directory Domain Services installation process starts.

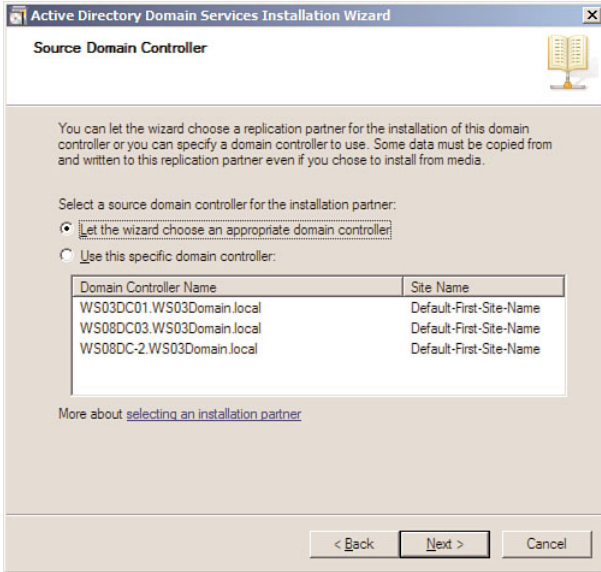


FIGURE 3.49

The Source Domain Controller page.

16. After the installation is complete, the Completing the Active Directory Domain Services Installation Wizard page appears. Ensure the installation was successful and click Finish.
17. When prompted to restart, click Restart Now.
18. To validate the installation process, click Start, click Run, type **C:\Windows\Debug**, and click OK.
19. Open the DCPROMO.log file and analyze the results in the file.

Remove a Domain Controller from a Domain

Scenario/Problem: A domain controller that is located in one of your offices is no longer required.

Solution: Remove the domain controller from the domain.

To remove a domain controller from a domain, perform the following steps using an AD DS account that has membership in the following AD DS group:

- ▶ Domain Admins

1. Log on to the domain controller you want to remove from the domain.
2. Click Start, click Run, type **dcpromo**, and click OK.
3. On the Welcome to the Active Directory Domain Services Installation Wizard page, click Next.
4. If the domain controller is a global catalog server, a message appears to warn you about the effect of removing a global catalog server from the environment, as shown in Figure 3.50. Click OK to continue.

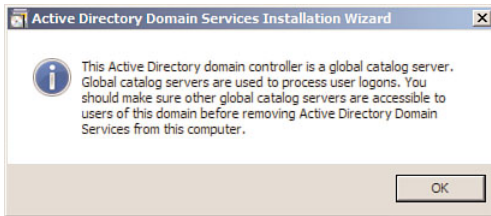


FIGURE 3.50
Global catalog warning.

5. On the Delete the Domain page, make no selection if this is not the last domain controller in the domain. If you do want to delete the domain, select the option to delete the domain and click Next.
6. On the Administrator Password page, type and confirm a secure password for the local Administrator account; then click Next.
7. On the Summary page, click Next.
8. The Active Directory Domain Services Installation Wizard deletes AD DS from the server.
9. On the Completing the Active Directory Domain Services Installation Wizard page, click Finish. Then reboot the server.

Forcing the Removal of a Windows Server 2008 Domain Controller

Scenario/Problem: You are forced into a situation where you cannot gracefully uninstall Active Directory Domain Services from a DC.

Solution: In Windows Server 2008, you can forcefully remove a DC when it is started in Directory Services Restore Mode. Typically, you force the removal of a DC only if the DC has no connectivity with other DCs.

Because the DC cannot contact other DCs during the operation, the AD DS forest metadata is not automatically updated as it is when a DC is removed normally. Instead, you must manually update the forest metadata after you remove the DC.

To force the removal of a Windows Server 2008 DC, perform the following steps:

1. Log on to the server using the Directory Services Restore Mode Administrator account.
2. Click Start, click Run, type `dcpromo /forceremoval`, and press ENTER.
3. On the Welcome to the Active Directory Domain Services Installation Wizard page, click Next.
4. On the Force the Removal of Active Directory Domain Services page, click Next.
5. On the Administrator Password page, type and confirm a password for the local Administrator account; then click Next.
6. On the Summary page, click Next.
7. Restart the server after the removal is complete.

Performing Metadata Cleanup

Scenario/Problem: You forced the removal of a DC, but data is lingering in AD DS. You need to remove this lingering data.

Solution: To remove lingering objects from AD DS after a forceful removal of a DC, you must perform metadata cleanup.

To perform a metadata cleanup, perform the following steps:

1. Log on to a writable domain controller.
2. Click Start, click Administrative Tools, and click Active Directory Users and Computers.
3. In the Active Directory Users and Computers console, select the Domain Controllers Organizational Unit (OU).
4. Right-click the domain controller you want to remove from the metadata, and select Delete.
5. On the dialog box to confirm the computer object deletion, shown in Figure 3.51, click Yes.

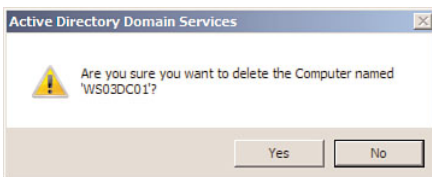


FIGURE 3.51
Confirming computer deletion.

6. On the Deleting Domain Controller dialog box, shown in Figure 3.55, select the option This Domain Controller is permanently offline and can no longer be demoted using the Active Directory Domain Services Installation Wizard (DCPROMO). Then click Delete.

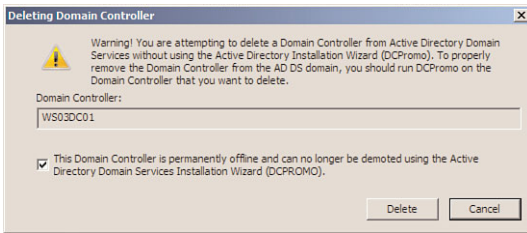


FIGURE 3.55
The Deleting Domain Controller dialog box.

7. If the domain controller was also a global catalog server, you receive an additional prompt asking whether you want to continue, as shown in Figure 3.56; click Yes.

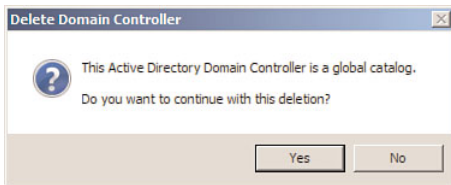


FIGURE 3.56
Global catalog deletion confirmation.

8. If the domain controller holds any operations master roles, an additional prompt displays. Click OK to move the roles to the server(s) DCPROMO recommends, or click Cancel and move the roles manually.
9. The Active Directory Domain Users and Computers console cleans all metadata for the DC.

Rename a Domain Controller

Scenario/Problem: The name of a DC is taken from the name of the member server during the installation of AD DS. In some cases, you might need to change the name of the DC after AD DS has been installed.

Solution: The netdom command-line tool can be used to rename a Windows Server 2008 DC.

To rename a domain controller, perform the following steps using an AD DS account that has membership in one of the following AD DS groups:

- ▶ Domain Admins
 - ▶ Enterprise Admins
1. Log on to the domain controller you want to rename.
 2. Click Start and click Command Prompt.
 3. In the Command Prompt window, type **netdom computername CurrentComputerName /add:NewComputerName**, where CurrentComputerName is the current FQDN name and NewComputerName is the new FQDN name. Then press ENTER.
 4. Ensure the computer account updates and DNS registrations are completed. In the Command Prompt window, type **netdom computername CurrentComputerName /makeprimary:NewComputerName**, where CurrentComputerName is the current FQDN name and NewComputerName is the new FQDN name. Then press ENTER.
 5. In the Command Prompt window, type **netdom computername NewComputerName /remove:OldComputerName**, where CurrentComputerName is the current FQDN name and NewComputerName is the new FQDN name. Then press ENTER.

Index

A

account lockout policies

PSO

- applying to users/groups, 412
- creating, 402, 405-409
- deleting, 410
- modifying defined settings in, 411
- modifying precedence of, 414
- viewing defined settings in, 410
- viewing resultant PSO for users/groups, 415

- shadow groups, creating, 416

account properties, modifying (user objects), 258

accounts (user), copying, 246

ACE (Access Control Entry), adding to ACL (Access Control Lists), 165

Active Directory Sites and Services

- Find feature, 181, 184, 187-189, 193
- Inter-Site Transports node, 167
- site properties page
 - Attribute Editor tab, 166, 172
 - General tab, 163-164, 171
 - Location tab, 164
 - Object tab, 165, 172
 - Security tab, 165, 172

Active Directory Users and Computers, accessing AD DS snapshot data, 453

AD DS (Active Directory Domain Services)

- auditing, 6
 - configuring on object SACL, 470
- Detailed Directory Service
 - Replication auditing subcategory, 468-469
- Directory Service Changes auditing subcategory, 464-465
- Directory Service Replication auditing subcategory, 466-468

- excluding attributes from, 473
 - Global Audit Policy, 456-461
 - state of directory service access auditing subcategories, 461-463
- child domains, installing, 38
 - answer files, 46-49
 - command line, 44-46
 - Windows interface, 39-43
- database mining tool, 7
- DC
 - installing, 58-63
 - removing, 73
- domain trees, installing via
 - answer files, 55-57
 - command line, 53-55
 - Windows interface, 50-52
- forests, installing via
 - answer files, 36-37
 - command line, 32-33, 35
 - Windows interface, 24-28, 31
- installing
 - domain installations, 18-19
 - forest installations, 14-16
 - media, 70-71
 - restored backup media, 68
- metadata cleanups, 74-75
- new features of, 6-7
- password policies, 6
- restarting, 7
- RODC, 6
 - account creation, 64-66
 - attaching servers to RODC accounts, 67
 - domain installations, 20-21
- Schema
 - activating attributes, 216
 - activating classes, 231-232
 - adding attributes to ANR filters, 219
 - adding attributes to global catalog replication, 221-222
 - applying administrative permissions, 210
 - configuring attribute ranges, 227-228
 - configuring attributes for duplicating users, 223-224
 - configuring class attributes, 236
 - configuring class relationships, 235
 - configuring classes in Advanced view, 233-234
 - configuring Schema class attributes, 236
 - creating attributes, 213
 - creating classes, 228-229
 - creating shortcuts for, 209
 - deactivating attributes, 215
 - deactivating classes, 230
 - indexing attributes, 217-218, 225-227
 - installing, 206-207
 - removing attributes from ANR filters, 220
 - removing attributes from global catalog replication, 222-223
 - string syntax in attributes, 219
 - viewing attribute definitions, 212
 - viewing class definitions, 212
- sites
 - associating sites with links, 174
 - configuring link properties, 170-172
 - configuring properties of, 163-166
 - creating, 156
 - creating links, 166-167
 - creating site link bridges, 175
 - deleting, 159
 - deleting links, 170
 - deleting site link bridges, 178
 - disabling DC as bridgehead servers, 186-187
 - disabling KCC, 193-194
 - enabling DC as bridgehead servers, 183-185
 - enabling KCC, 196
 - moving DC between sites, 181-182
- snapshots
 - accessing data via Active Directory Users and Computers, 453

- accessing data via LDP.exe, 452-453
- creating onetime snapshots, 447
- creating scheduled snapshots, 448-449
- exposing snapshots as LDAP servers, 451
- subnets
 - adding, 178-179
 - deleting, 180-181
- address properties, modifying (user objects), 257**
- administrative permissions, applying to Schema (AD DS), 210**
- Advanced view, configuring Schema classes, 233-234**
- Advertising tests (DC), 136**
- all site links option (bridges), 200-201**
- Allowed list, moving RODC authenticated accounts to, 395-397**
- ANR (ambiguous name resolution) filters, adding/removing Schema attributes, 219-220**
- answer files, installing**
 - child domains, 46-49
 - DC, 62-63
 - domain trees, 55-57
 - forests, 36-37
- Attribute Editor tab (Active Directory Sites and Services, site properties page), 166, 172**
- attributes**
 - custom attributes, modifying
 - computer objects, 313
 - group objects, 295
 - OU, 325
 - user objects, 278
 - Schema attributes
 - activating, 216
 - ANR filters, 219-220
 - class attribute configuration 236
 - creating, 213
 - deactivating, 215
 - duplicating users, 223-224
 - global catalog replication, 221-223

- indexing, 217-218, 225-227
- range configuration, 227-228
- string syntax in, 219
- viewing definitions, 212

auditing

- AD DS, 6
- Detailed Directory Service Replication auditing subcategory, 468-469
- Directory Service Changes auditing subcategory, 464-465
- Directory Service Replication auditing subcategory, 466-468
- excluding attributes from, 473
- Global Audit Policy
 - disabling via command line, 460-461
 - disabling via Windows interface, 459-460
 - enabling via Windows interface, 456-459
- object SACL, configuring on, 470
- state of directory service access auditing subcategories
 - disabling, 463
 - enabling, 462
 - retrieving, 461
- authentication, configuring in trusts, 112-113**
- authoritative restores, AD DS, 436-438, 440**
- automatically populating migration tables, 350**

B

backups

- DC
 - critical volumes, 420-433
 - system state, 425
- GPO 338
- restored backup media, AD DS installations via, 68
- starter GPO, 338
- Windows Server Backup server feature
 - DC critical volume backups, 420-424

- DC full server backups, 426-433

- DC system state backups, 425

- installing, 418

block inheritance, GPO, 357-358

bridgehead servers

- configuring, 183

- DC as preferred bridgehead servers, 183-187

bridges

- all site links option, 200-201

- site link bridges, 175, 178

C

caching

- RODC password caches, pre-populating, 397-398

- universal group memberships, 160-162

child domains, installing via

- answer files, 46-49

- command line, 44-46

- Windows interface, 39-43

classes (Schema)

- activating, 231-232

- Advanced view, configuring in, 233-234

- attributes, configuring, 236

- creating, 228-229

- deactivating, 230

- definitions, viewing, 212

- relationships, configuring, 235

cmsDS-PasswordHistoryLength attribute (PSO), 405

cn attribute (PSO), 403

COM+ properties, modifying

- OU, 323

- user objects, 272

command line

- child domains, installing, 44-46

- computer objects

- adding to groups, 303

- creating, 298

- deleting, 299

- disabling, 304

- enabling, 306

- moving, 301-302

DC

- backups, 424, 428, 431-433

- full server recovery, 443-446

- installing, 60-61

- domain naming master roles, transferring via, 141

- domain trees, installing, 53-55

- forests, installing, 32-35

- Global Audit Policies, 458-461

- global catalog roles, 126-128

- group objects

- adding to groups, 287

- creating, 280

- deleting, 281

- moving, 285

- renaming, 283-284

- infrastructure master roles, transferring via, 147

OU

- creating, 315

- deleting, 317

- moving, 319

- renaming, 318

- PDC emulator roles, transferring via, 146

- RID master roles, transferring via, 144

- schema master roles, transferring via, 139

- user objects

- adding to groups, 250

- creating, 241

- deleting, 242-243

- disabling, 252

- enabling, 253

- moving, 248

- renaming, 244-245

- resetting passwords, 255

comments, GPO, 336

computer objects

- creating, 296-298

- custom attributes, modifying, 313

- delegation properties, modifying, 309
- deleting, 299
- disabling, 304
- enabling, 305-306
- general properties, modifying, 307
- groups, adding to, 302-303
- location properties, modifying, 310
- Managed By properties, modifying, 311-312
- moving, 300-302
- operating system properties, modifying, 308
- password replication policies, viewing, 310
- protection from deletion properties, modifying, 312

computers, Password Replication Policies, 390-392

configuring

- AD DS site properties, 163-166, 170-172
- bridgehead servers, 183
- domain functional levels, 118-119
- forest functional levels, 119-121
- object SACL, auditing on, 470
- Schema class
 - Advanced view, 233-234
 - attributes, 236
 - relationships, 235
- trust authentication, 112-113

connection objects, 189, 192

containerized searches, indexing for Schema attributes, 225-227

copying

- GPO, 334-335
- passwords, viewing replication policies applied to
 - computer objects, 310
 - user objects, 276
- starter GPO, 334-335
- user accounts, 246
- user objects, 246
- WMI filters, 367

D

data recovery

AD DS

- accessing snapshot data via Active Directory Users and Computers, 453
- accessing snapshot data via LDP.exe, 452-453
- authoritative restores, 436-440
- creating onetime snapshots, 447
- creating scheduled snapshots, 448-449
- exposing snapshots as LDAP servers, 451
- nonauthoritative restores, 433-435

DC, full server recovery, 441-446

Windows Server Backup server feature

- DC critical volume backups, 420-424
- DC full server backups, 426-433
- DC system state backups, 425
- installing, 418

data restoration, AD DS

- authoritative restores, 436-440
- nonauthoritative restores, 433-435

database mining tool (AD DS), 7

DC (domain controllers)

- advertising, validating, 136
- backups
 - critical volumes, 420-424
 - full server backups, 426-433
 - system state, 425
- bridgehead servers, 183-187
- domain naming master roles
 - seizing, 149
 - transferring via command line, 141
 - transferring via Windows, 140
- domains, removing from, 72-73
- DSRM, restarting in, 433, 436
- global catalog roles, 124-128
- infrastructure master roles
 - seizing, 152-153
 - transferring via command line, 147
 - transferring via Windows, 146-147

- installing via
 - answer files, 62-63
 - command line, 60-61
 - Windows interface, 58-60
- manual connection objects
 - creating, 189
 - deleting, 192
- operations master role holders, identifying via
 - Dsquery, 134
 - Netdom, 135
- PDC emulator roles
 - seizing, 151-152
 - transferring via command line, 146
 - transferring via Windows, 145
- recovery (full server), 441-446
- removing, 73
- renaming, 75-76
- replication
 - manual connection objects, 189, 192
 - inbound replication, 196-197
 - outbound replication, 198-199
- RID master roles
 - seizing, 150
 - transferring via command line, 144
 - transferring via Windows, 142-144
- RODC
 - account creation in AD DS, 64-66
 - attaching servers to RODC
 - accounts, 67
 - installing, 64-67
- schema master roles
 - seizing, 148
 - transferring via command line, 139
 - transferring via Windows, 137
- sites, moving between, 181-182
- static IP addresses, assigning to, 26
- delegation properties, modifying (computer objects), 309**
- deleting**
 - AD DS sites, 159
 - computer objects, 299
 - DC from domains, 72-73
 - GPO, 330
 - group objects, 281
 - manual connection objects, 192
 - OU, 316-317
 - PSO, 410
 - site link bridges, 178
 - starter GPO, 332
 - subnets, 180-181
 - user objects, 242-243
- Detailed Directory Service Replication auditing subcategory, 468-469**
- dial-in properties, modifying (user objects), 267-268**
- direct reports (user objects), viewing, 265**
- Directory Service Changes auditing subcategory, 464-465**
- Directory Service Replication auditing subcategory, 466-468**
- disabling**
 - computer objects, 304
 - Detailed Directory Service Replication auditing subcategory, 469
 - Directory Service Changes auditing subcategory, 465
 - Directory Service Replication auditing subcategory, 467-468
 - Global Audit Policies
 - command line, 460-461
 - Windows interface, 459-460
 - GPO computer settings, 363
 - GPO links, 353
 - GPO user settings, 362
 - state of directory service access auditing subcategories, 463
 - user objects, 251-252
- disk space, Windows Server 2008 system requirements, 7**
- DNS, verifying global catalog registrations, 130**
- domain controllers. See DC (domain controllers)**
- domain naming master roles**
 - seizing, 149

- transferring via
 - command line, 141
 - Windows, 140

Domain Services. See AD DS (Active Directory Domain Services)

domain trees, installing via

- answer files, 55-57
- command line, 53-55
- Windows interface, 50-52

domains

- AD DS installations, 18-19
- DC, removing from, 72-73
- functional levels, configuring, 118-119
- global catalog servers, identifying in, 133
- RODC installations, 20-21

DS (Domain Services)

- sites
 - associating sites with links, 174
 - configuring link properties, 170-172
 - configuring properties of, 163-166
 - creating, 156
 - creating links, 166-167
 - creating site link bridges, 175
 - deleting, 159
 - deleting links, 170
 - deleting site link bridges, 178
 - disabling DC as bridgehead servers, 186-187
 - disabling KCC, 193-194
 - enabling DC as bridgehead servers, 183-185
 - enabling KCC, 196
 - moving DC between sites, 181-182

subnets

- adding, 178-179
- deleting, 180-181

dsmod command, 303-306

- renaming
 - group objects, 283
 - user objects, 244
- shadow groups, creating, 416

dsmove command, 301

- group objects
 - moving, 285
 - renaming, 284
- user objects, renaming, 244-245

Dsquery, identifying operations master role holders, 134

DSRM, restarting in DC, 433, 436

duplicating users, configuring Schema attributes for, 223-224

E - F

editing

- GPO, 333-334
- starter GPO, 333-334

Enable Universal Group Membership Caching (NTDS Site Settings Properties page), 161

environment properties, modifying (user objects), 268

exporting

- starter GPO, 343
- WMI filters, 366

external trusts, 90

- one-way trusts, creating
 - creating incoming forest trusts, 95-97
 - creating outgoing forest trusts, 99-100
- two-way trusts, creating, 91-95

filters

- ANR filters, adding/removing Schema attributes, 219-220
- GPO scope, filtering via security groups, 360
- WMI filters
 - copying, 367
 - creating, 364
 - exporting, 366
 - GPO delegated permissions and, 385-387
 - importing, 365
 - linking to GPO, 367

Find feature (Active Directory Sites and Services), 181, 184, 187-189, 193

fine-grained password policies

PSO

- applying to users/groups, 412
- creating, 402, 405-409
- deleting, 410
- modifying defined settings in, 411
- modifying precedence of, 414
- viewing defined settings in, 410
- viewing resultant PSO for users/groups, 415

shadow groups, creating, 416

forest trusts, name suffixes

local forests, excluding from routing to, 111-112

routing

- changing status, 107-108
- enabling/disabling from, 109-110

forests

AD DS installations, 14-16

functional levels, configuring, 119-121

global catalog servers, identifying in, 132

installing via

- answer files, 36-37
- command line, 32-35
- Windows interface, 24-31

one-way trusts

- incoming external trusts, 95-97
- incoming trusts, 82, 85
- outgoing external trusts, 99-100
- outgoing trusts, 87, 90

two-way trusts, creating, 78, 81

user principal names, adding to/
removing from, 116-117

functional levels (AD DS), 28

G

general properties, modifying

- computer objects, 307
- group objects, 288

OU, 321

user objects, 256

General tab (Active Directory Sites and Services, site properties page), 163-164, 171

Global Audit Policies, enabling/disabling via

command line, 458-461

Windows interface, 456-460

global catalog replication, adding/removing Schema attributes, 221-223

global catalog servers

identifying in

- domains, 133
- forests, 132

roles

- disabling, 126-128
- enabling, 124-126

verifying

- DNS registrations, 130
- readiness, 128-130

GPO (group policy objects), 456

backing up, 338

block inheritance in, 357-358

commenting, 336

computer settings, disabling, 363

copying, 334-335

creating, 329, 332-333

delegating permissions, 374

GPO links, 377-379

group policy modeling data, 380-382

group policy results, 383-385

modifying, 375

removing, 376

WMI filters, 385-387

deleting, 330

editing, 333-334

links

changing order of, 359

creating, 352

delegated permissions, 377-379

disabling, 353

- enabling, 354
- enforcing, 355
- removing, 353
- removing enforcement of, 356-357
- migration tables
 - automatically populating, 350
 - creating, 348-349
- reports, printing, 337
- restoring, 339-340
- resultant sets of policies
 - determining, 368-370
 - simulating, 370-372
- scope, filtering via security groups, 360
- searching, 345-346
- starter GPO
 - backing up, 338
 - commenting, 336
 - copying, 334-335
 - creating, 330
 - creating new GPO, 332-333
 - deleting, 332
 - editing, 333-334
 - exporting, 343
 - importing, 344
 - printing reports, 337
 - restoring, 339-340
 - saving reports, 337
 - viewing reports, 337
- user settings, disabling, 362
- WMI filters
 - copying, 367
 - creating, 364
 - delegated permissions and, 385-387
 - exporting, 366
 - importing, 365
 - linking to GPO, 367

group memberships

- modifying (user objects), 266
- universal caching, enabling/disabling, 160-162

group objects

- creating, 279-280
- custom attributes, modifying, 295
- deleting, 281
- general properties, modifying, 288
- groups, adding to, 286-287
- Managed By properties, modifying, 293
- members, modifying, 291
- moving, 285
- protection from deletion properties, modifying, 294
- renaming, 282-284
- scope, modifying, 289-290
- type, modifying, 290

group policies, GPO delegated permissions and, 380-385

groups

- computer objects, adding to, 302-303
- group objects, adding to, 286-287
- Password Replication Policies, adding to/removing from, 390-392
- PSO
 - applying to, 412
 - viewing resultant PSO, 415
- user objects, adding, 249-250

H - I

hard disks, Windows Server 2008 system requirements, 7

importing

- starter GPO, 344
- WMI filters, 365

inbound replication, 196-197

indexing Schema attributes, 217

- containerized searches, 225-227
- removing attributes from indexes, 218

infrastructure master roles

- seizing, 152-153
- transferring via
 - command line, 147
 - Windows, 146-147

inheritance (block), GPO, 357-358

Initial Configuration Tasks page (Windows Server 2008 installation), 11

installing

AD DS

domain installations, 18-19

forest installations, 14-16

media, 70-71

restored backup media, 68

child domains, 38

answer files, 46-49

command line, 44-46

Windows interface, 39-43

DC

answer files, 62-63

command line, 60-61

Windows interface, 58-60

domain trees

answer files, 55-57

command line, 53-55

Windows interface, 50-52

forests

answer files, 36-37

command line, 32-35

Windows interface, 24-28, 31

Netdom command-line tool, 14

RODC, 64-67

Schema (AD DS), 206-207

Windows Server 2008

Initial Configuration Tasks page, 11

language selection, 8

passwords, 11

Select the Operating System You
Want to Install page, 9

Server Manager configuration, 12

Where Do You Want to Install
Windows? page, 9

Which Type of Installation Do You
Want? page, 9

Windows Server Backup server
feature, 418

Inter-Site Transports node (Active Directory Sites and Services), 167

IP addresses, DC assignments, 26

J - K - L

KCC (Knowledge Consistency Checker),
enabling/disabling for sites, 193-196

languages, selecting for Windows Server
2008 installations, 8

LDAP servers, exposing AD DS snapshots
as, 451

LDP, verifying global catalog server
readiness, 129

LDP.exe, accessing AD DS snapshot data
via, 452-453

links

AD DS sites

associating sites with links, 174

configuring link properties, 170-172

creating for, 166-167

creating site link bridges, 175

deleting from, 170

deleting site link bridges, 178

GPO

changing link order in, 359

creating for, 352

delegated permissions, 377-379

disabling, 353

enabling, 354

enforcing, 355

removing, 353

removing enforcement of, 356-357

WMI filter links to GPO, 367

list vol Dispart command, 445

location properties, modifying

computer objects, 310

Location tab (Active Directory Sites
and Services, site properties page),
164

lockout policies (account)

PSO

applying to users/groups, 412

creating, 402, 405-409

deleting, 410

modifying defined settings in, 411

modifying precedence of, 414

viewing defined settings in, 410

viewing resultant PSO for users/groups, 415

shadow groups, creating, 416

logon hours, modifying (user objects), 259

M

Managed By properties, modifying

computer objects, 311-312

group objects, 293

OU, 322

manual connection objects

creating, 189

deleting, 192

maximum acceptable values (ranges), 228

members, modifying in group objects, 291

memory, Windows Server 2008 system requirements, 7

metadata cleanups, 74-75

migration tables

automatically populating, 350

creating, 348-349

minimum acceptable values (ranges), 228

moving

computer objects, 300-302

group objects, 285

OU, 319

RODC authenticated accounts to Allowed list, 395-397

user objects, 248

msDS-LockoutDuration attribute (PSO), 408

msDS-LockoutObservationWindow attribute (PSO), 408

msDS-LockoutThreshold attribute (PSO), 407

msDS-MaximumPasswordAge attribute (PSO), 407

msDS-MinimumPasswordAge attribute (PSO), 406

msDS-MinimumPasswordLength attribute (PSO), 406

msDS-PasswordComplexityEnabled attribute (PSO), 405

msDS-PasswordReversibleEncryptionEnabled attribute (PSO), 404

msDS-PasswordSettingsPrecedence attribute (PSO), 403

N

name suffix routing, forest trust name suffixes

local forests, excluding suffixes from routing to, 111-112

routing

changing status of, 107-108

enabling/disabling from, 109-110

naming

DC, 75-76

group objects, 282-284

OU, 318

user objects, 243-245

Netdom command-line tool

installing, 14

operations master role holders, identifying via, 135

NLTest, verifying readiness of global catalog servers, 130

nonauthoritative restores, AD DS, 433-435

NTDS Site Settings Properties page, Enable Universal Group Membership Caching, 161

O

object SACL (security access control lists)

auditing, configuring, 470

Object tab (Active Directory Sites and Services, site properties page), 165, 172

one-way trusts

defining, 78

external trusts

creating incoming forest trusts, 95-97

creating outgoing forest trusts, 99-100

forests trusts

- incoming external trusts, 95-97
- incoming trusts, 82, 85
- outgoing external trusts, 99-100
- outgoing trusts, 87, 90

operating system properties, modifying (computer objects), 308**operations master role holders, identifying via**

- Dsquery, 134
- Netdom, 135

organization properties, modifying (user objects), 263**OU (organizational units)**

- COM+ properties, modifying, 323
- creating, 314-315
- custom attributes, modifying, 325
- deleting, 316-317
- general properties, modifying, 321
- Managed By properties, modifying, 322
- moving, 319
- protection from deletion properties, modifying, 324
- renaming, 318

outbound replication, 198-199**P****passwords**

- AD DS policies, 6
- fine-grained password policies
 - applying PSO to users/groups, 412
 - creating PSO, 402, 405-409
 - creating shadow groups, 416
 - deleting PSO, 410
 - modifying defined PSO settings, 411
 - modifying PSO precedence, 414
 - viewing defined PSO settings, 410
 - viewing resultant PSO for users/groups, 415
- Password Settings Containers, 19
- PSO, 6

replication policies, 390

- adding to/removing from computers, 390-392
- adding to/removing from groups, 390-392
- adding to/removing from users, 390-392
- pre-populating RODC password caches, 397-398
- RODC authenticated accounts, 394-397
- RODC cached credentials, 393, 399-400
- viewing policies applied to computer objects, 310
- viewing policies applied to user objects, 276
- user objects, resetting in, 254-255
- Windows Server 2008 installations, 11

PDC emulator roles

- seizing, 151-152
- transferring via
 - command line, 146
 - Windows, 145

permissions

- administrative permissions, applying to Schema (AD DS), 210
- GPO delegated permissions, 374
- GPO links, 377-379
- group policy modeling data, 380-382
- group policy results, 383-385
- modifying, 375
- removing, 376
- WMI filters, 385-387

populating migration tables automatically, 350**printing GPO reports, 337****processors, Windows Server 2008 system requirements, 7****profile properties, modifying (user objects), 261****protection from deletion properties, modifying**

- computer objects, 312
- group objects, 294

OU, 324

user objects, 277

PSO (password settings objects), 6

cn attribute, 403

creating, 402, 405-409

defined settings

 modifying, 411

 viewing, 410

deleting, 410

groups

 applying to, 412

 viewing resultant PSO, 415

msDS-LockoutDuration attribute, 408

msDS-LockoutObservationWindow
attribute, 408

msDS-LockoutThreshold attribute, 407

msDS-MaximumPasswordAge attribute,
407

msDS-MinimumPasswordAge attribute,
406

msDS-MinimumPasswordLength
attribute, 406

msDS-PasswordComplexityEnabled
attribute, 405

msDS-PasswordHistoryLength
attribute, 405

msDS-
PasswordReversibleEncryptionEnable
d attribute, 404

msDS-PasswordSettingsPrecedence
attribute, 403

precedence, modifying, 414

shadow groups, creating, 416

users

 applying to, 412

 viewing resultant PSO, 415

published certificates properties, modifying (user objects), 273-274

Q - R

ranges

maximum acceptable values, 228

minimum acceptable values, 228

Schema attribute ranges, configuring,

227-228

realm trusts, creating, 103-104

recovery

AD DS

accessing snapshot data via Active
Directory Users and Computers,
453

accessing snapshot data via
LDP.exe, 452-453

authoritative restores, 436-440

creating onetime snapshots, 447

creating scheduled snapshots,
448-449

exposing snapshots as LDAP
servers, 451

nonauthoritative restores, 433-435

DC

critical volume backups, 420-424

full server backups, 426-433

full server recovery, 441-446

system state backups, 425

Windows Server Backup server feature

DC critical volume backups,
420-424

DC full server backups, 426-433

DC system state backups, 425

installing 418

remote control properties, modifying (user objects), 270-271

removing

block inheritance from GPO, 358

DC from domains, 72-73

GPO delegated permissions from, 376

 GPO links, 379

 group policy modeling data, 382

 group policy results, 385

 WMI filters, 386-387

GPO links, 353, 356-357

members from group objects, 291

Schema attributes from

 ANR filters, 220

 global catalog replication, 222-223

 indexes, 218

trusts, 115

user principal names from forests, 117

renaming

DC, 75-76

group objects, 282-284

OU, 318

user objects, 243-245

replication

bridge all site links option, 200-201

DC

manual connection objects, 189, 192

inbound replication, 196-197

outbound replication, 198-199

triggering, 203

verifying functioning of, 202

replication policies (passwords), viewing policies applied to

computer objects, 310

user objects, 276

reports (GPO), 337

requirements (system), Windows Server 2008, 7

restarting AD DS, 7

restored backup media, AD DS installations via, 68

restoring

data, AD DS

authoritative restores, 436-440

nonauthoritative restores, 433-435

GPO, 339-340

starter GPO, 339-340

resultant sets of policies (GPO)

determining, 368-370

simulating, 370-372

RID master roles

seizing, 150

transferring via

command line, 144

Windows, 142-144

RODC (read-only domain controllers), 6

account creation in AD DS, 64-66

authenticated accounts

moving to Allowed list, 395-397

reviewing, 394-395

cached credentials

resetting, 399-400

viewing, 393

domain installations, 20-21

installing, 64-67

password caches, pre-populating, 397-398

servers, attaching to RODC accounts, 67

roles

domain naming master roles

seizing, 149

transferring via command line, 141

transferring via Windows, 140

global catalog roles

disabling, 126-128

enabling, 124-126

infrastructure master roles

seizing, 152-153

transferring via command line, 147

transferring via Windows, 146-147

operations master role holders, identifying via

Dsquery, 134

Netdom, 135

PDC emulator roles

seizing, 151-152

transferring via command line, 146

transferring via Windows, 145

RID master roles

seizing, 150

transferring via command line, 144

transferring via Windows, 142, 144

schema master roles

seizing, 148

transferring via command line, 139

transferring via Windows, 137

S

saving GPO reports, 337**Schema (AD DS)**

- administrative permissions, applying, 210
- attributes
 - activating, 216
 - adding to ANR filters, 219
 - adding to global catalog replication, 221-222
 - configuring attribute ranges, 227-228
 - configuring Schema class attributes, 236
 - creating, 213
 - deactivating, 215
 - duplicating users, 223-224
 - indexing, 217-218, 225-227
 - removing from ANR filters, 220
 - removing from global catalog replication, 222-223
 - string syntax in, 219
 - viewing definitions of, 212

classes

- activating, 231-232
- configuring attributes of, 236
- configuring in Advanced view, 233-234
- configuring relationships, 235
- creating, 228-229
- deactivating, 230
- viewing definitions of, 212

installing, 206-207

shortcuts, creating, 209

schema master roles

- seizing, 148
- transferring via
 - command line, 139
 - Windows, 137

scope

- GPO scope, filtering via security groups, 360
- group objects, modifying in, 289-290

searches

- containerized searches, indexed Schema attributes, 225-227

GPO, 345-346

security groups filtering via GPO scope, 360**Security tab (Active Directory Sites and Services, site properties page), 165, 172****Select the Operating System You Want to Install page (Windows Server 2008 installation), 9****Server Manager, Windows Server 2008 installations, 12****servers**

bridgehead servers

configuring, 183

disabling DC as preferred bridgehead servers, 186-187

enabling DC as preferred bridgehead servers, 183-185

global catalog servers

disabling roles, 126-128

enabling roles, 124-126

identifying in domains, 133

identifying in forests, 132

verifying DNS registrations, 130

verifying readiness, 128-130

RODC accounts, attaching to, 67

sessions properties, modifying (user objects), 269**shadow groups, creating, 416****shortcut trusts, creating, 106-107****site properties page (Active Directory Sites and Services)**

Attribute Editor tab, 166, 172

General tab, 163-164, 171

Location tab, 164

Object tab, 165, 172

Security tab, 165, 172

sites (AD DS)

configuring properties of, 163-166

creating, 156

DC

disabling DC as bridgehead servers, 186-187

enabling DC as bridgehead servers, 183-185

moving between sites, 181-182

deleting, 159

KCC

disabling, 193-194

enabling, 196

links

associating sites with links, 174

configuring properties, 170-172

creating, 166-167

creating site link bridges, 175

deleting, 170

deleting site link bridges, 178

snapshots (AD DS)

accessing data via

Active Directory Users and
Computers, 453

LDP.exe, 452-453

LDAP servers, exposing snapshots as,
451

onetime snapshots, creating, 447

scheduled snapshots, creating,
448-449

starter GPO (group policy objects)

backing up, 338

commenting, 336

copying, 334-335

creating, 330

deleting, 332

editing, 333-334

exporting, 343

importing, 344

new GPO, creating, 332-333

reports, printing, 337

restoring, 339-340

state of directory service access auditing subcategories

disabling, 463

enabling, 462

retrieving, 461

static IP addresses, DC assignments, 26

subnets, AD DS

adding to, 178-179

deleting from, 180-181

syntax

string syntax, Schema attributes and,
219

System containers, 18

system requirements, Windows Server 2008, 7

T

telephone properties, modifying (user objects), 262

Terminal Services properties, modifying (user objects), 271

trusts

authentication scope, configuring,
112-113

defining, 78

external trusts, 90

creating one-way external trusts,
95-100

creating two-way trusts, 91-95

forest trusts

changing name suffix routing
status, 107-108

enabling/disabling name suffixes
from routing, 109-110

excluding name suffixes from
routing to local forests, 111-112

one-way trusts

creating incoming external forest
trusts, 95-97

creating incoming external trusts,
95-97

creating incoming forest trusts, 82,
85

creating outgoing external forest
trusts, 99-100

creating outgoing external trusts,
99-100

creating outgoing forest trusts, 87,
90

defining, 78

realm trusts, creating, 103-104

removing, 115

shortcut trusts, creating, 106-107

two-way trusts

creating external trusts, 91-95

creating forest trusts, 78, 81

defining, 78

validating, 113-115

type, modifying in group objects, 290

U

universal group membership caching, 160-162

unscheduled backups, DC

critical volumes, 420-424

full server backups, 426-428

system state, 425

user accounts, copying, 246

user duplication, configuring for Schema attributes, 223-224

user objects

account properties, modifying, 258

address properties, modifying, 257

COM+ properties, modifying, 272

computers users can log on to, modifying, 260

copying, 246

creating, 239-241

custom attributes, modifying, 278

deleting, 242-243

dial-in properties, modifying, 267-268

direct reports, viewing, 265

disabling, 251-252

enabling, 253

environment properties, modifying, 268

general properties, modifying, 256

groups

adding to, 249-250

modifying memberships, 266

logon hours, modifying, 259

managers, modifying, 264

moving, 248

organization properties, modifying, 263

passwords

resetting, 254-255

viewing replication policies, 276

profile properties, modifying, 261

protection from deletion properties, modifying, 277

published certificates properties, modifying, 273-274

remote control properties, modifying, 270-271

renaming, 243-245

sessions properties, modifying, 269

telephone properties, modifying, 262

Terminal Services properties, modifying, 271

user principal names, adding to/removing from forests, 116-117

user's managers, modifying, 264

users

Password Replication Policies, adding to/removing from, 390-392

PSO

applying to, 412

viewing resultant PSO, 415

V - W - X - Y - Z

validating trusts, 113-115

Where Do You Want to Install Windows? page (Windows Server 2008 installation), 9

Which Type of Installation Do You Want? page (Windows Server 2008 installation), 9

Windows interface

child domains, installing, 39-43

computer objects

adding to groups, 302

creating, 296-298

deleting, 299

disabling, 304

enabling, 305

- moving, 300
- DC
 - backups, 420-423, 426-431
 - full server recovery, 441-443
 - installing, 58-60
 - domain naming master roles, transferring via, 140
 - domain trees, installing, 50-52
 - forests, installing, 24-28, 31
 - Global Audit Policies
 - disabling, 459-460
 - enabling, 456-457
 - global catalog roles
 - disabling, 126-127
 - enabling, 124-125
 - group objects
 - adding to groups, 286
 - creating, 279
 - deleting, 281
 - moving, 285
 - renaming, 282
 - infrastructure master roles, transferring via, 146-147
 - OU
 - creating, 314-315
 - deleting, 316
 - moving, 319
 - renaming, 318
 - PDC emulator roles, transferring via, 145
 - RID master roles, transferring via, 142-144
 - schema master roles, transferring via, 137
 - user objects
 - adding to groups, 249
 - creating, 239-240
 - deleting, 242
 - disabling, 251
 - enabling, 253
 - moving, 248
 - renaming, 243
 - resetting passwords, 254
- Windows Server 2008**
 - child domains, installing via, 38
 - answer files, 46-49
 - command line, 44-46
 - Windows interface, 39-43
 - DC
 - installing via, 58-63
 - removing, 73
 - domain trees, installing via
 - answer files, 55-57
 - command line, 53-55
 - Windows interface, 50-52
 - forests, installing via
 - answer files, 36-37
 - command line, 32-35
 - Windows interface, 24-28, 31
 - installing
 - Initial Configuration Tasks page, 11
 - language selection, 8
 - passwords, 11
 - Select the Operating System You Want to Install page, 9
 - Server Manager configuration, 12
 - Where Do You Want to Install Windows? page, 9
 - Which Type of Installation Do You Want? page, 9
 - system requirements, 7
- Windows Server Backup server feature**
 - DC backups
 - critical volume backups, 420-424
 - full server backups, 426-433
 - system state backups, 425
 - installing, 418
- WMI filters**
 - copying, 367
 - creating, 364
 - exporting, 366
 - GPO delegated permissions and, 385-387
 - importing, 365
 - linking to GPO, 367