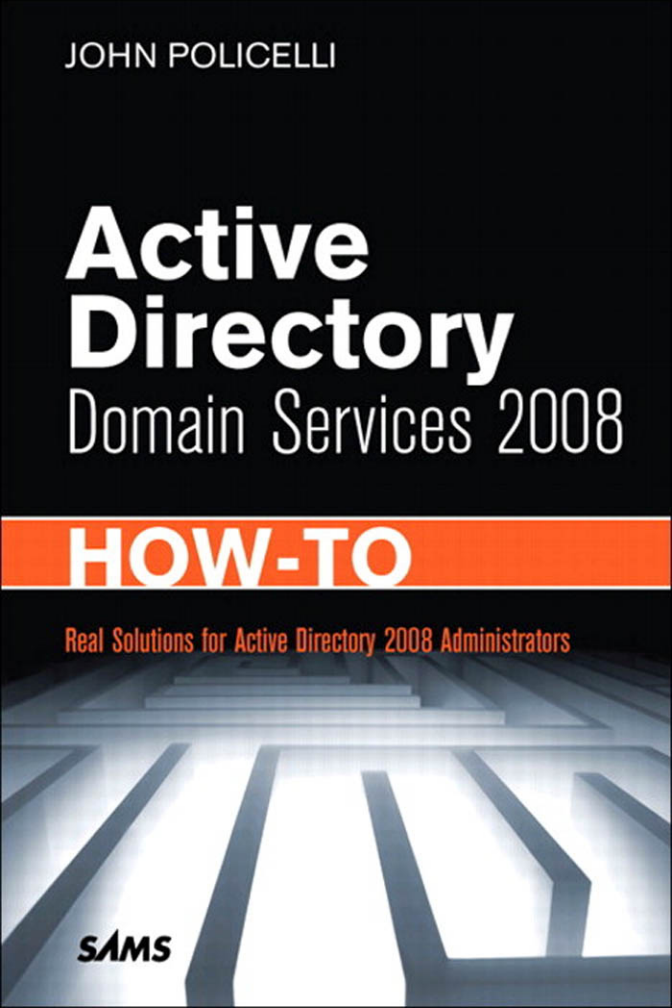
JOHN POLICELLI

Active Directory Domain Services 2008

HOW-TO

Real Solutions for Active Directory 2008 Administrators



SAMS

Active Directory Domain Services 2008 How-To

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

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).

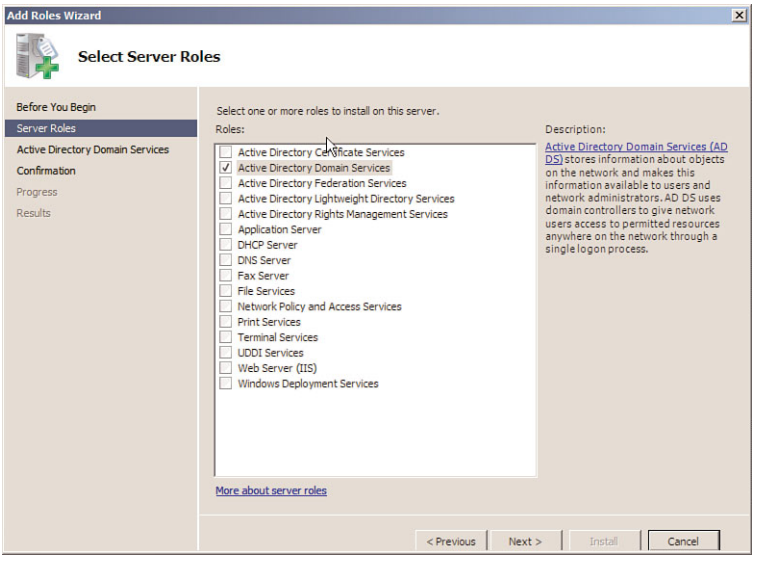


FIGURE 3.1
The Select Server Roles page.

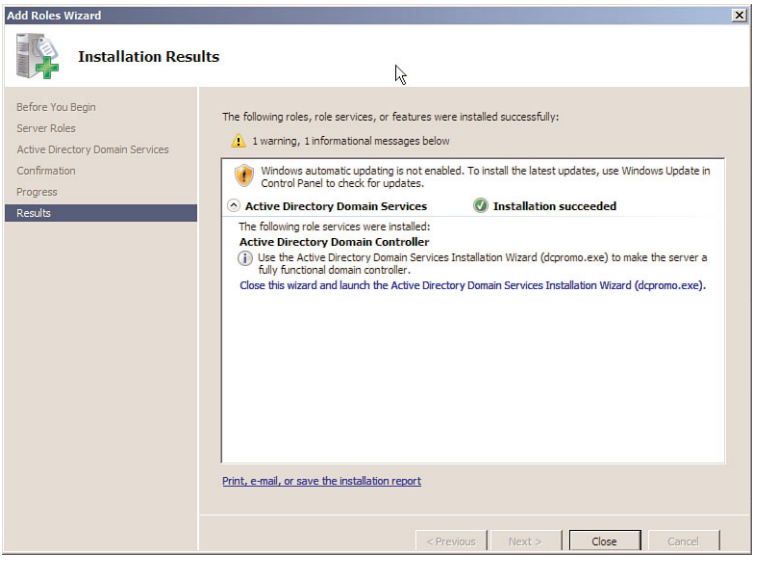


FIGURE 3.2
The Installation Results page.

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.

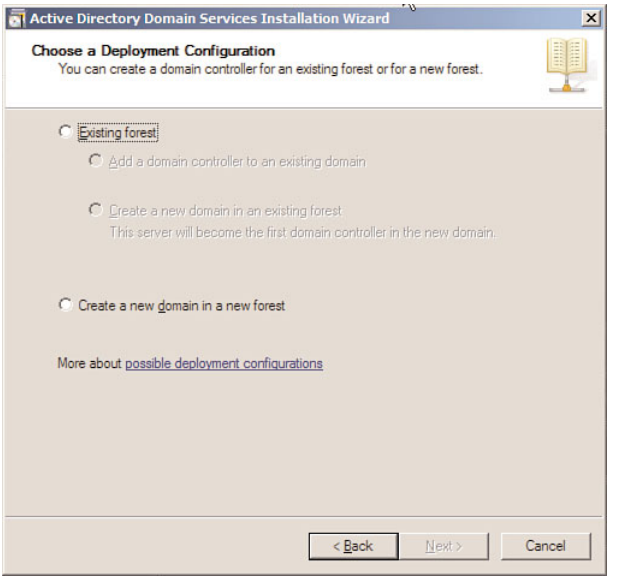


FIGURE 3.3
The Choose a Deployment Configuration page.

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.

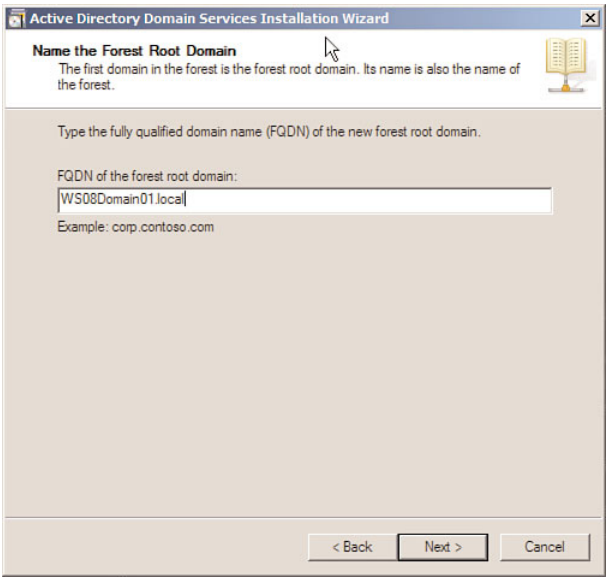


FIGURE 3.4
The Name the Forest Root Domain page.

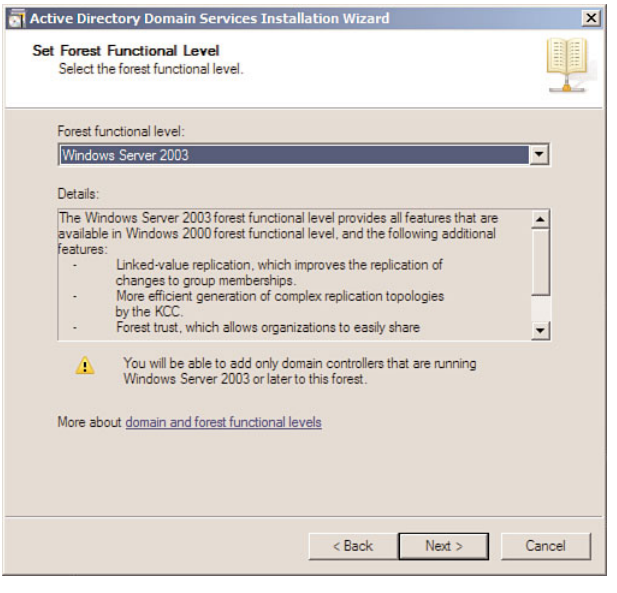


FIGURE 3.5
The Set Forest Functional Level page.

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.

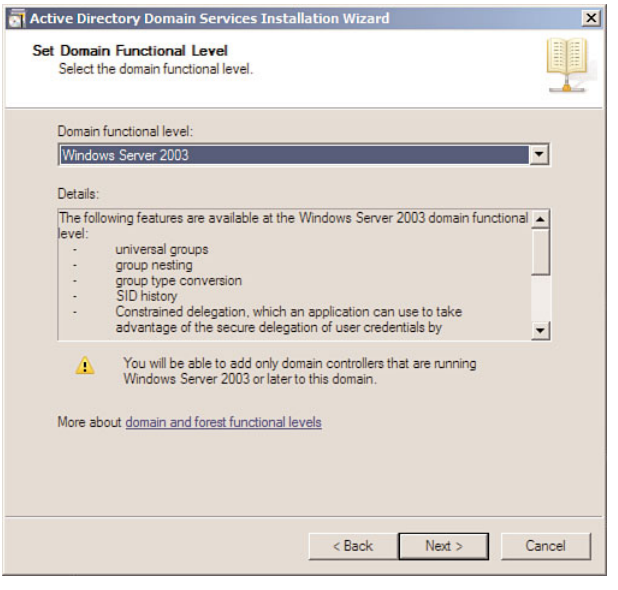


FIGURE 3.6
The Set Domain Functional Level page.

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.

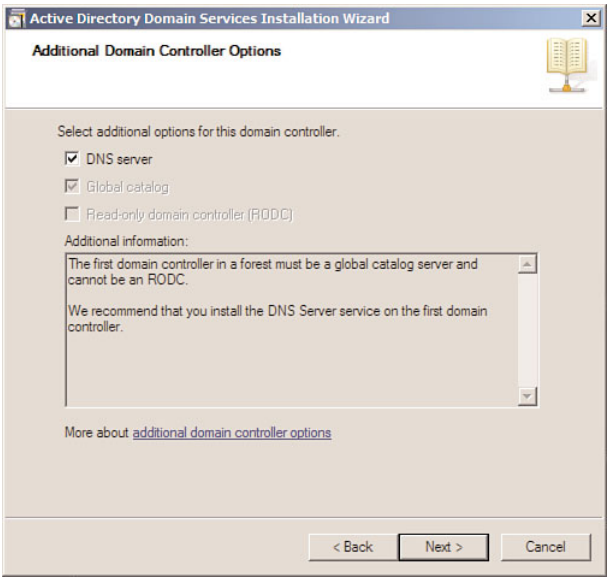


FIGURE 3.7
The Additional Domain Controller Options page.

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.

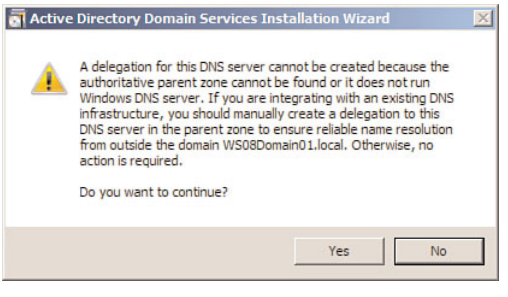


FIGURE 3.8
The manual DNS Delegation Message.

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.

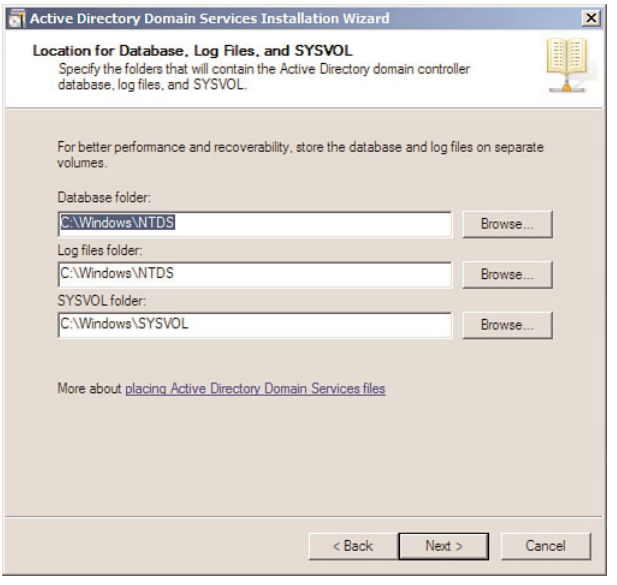


FIGURE 3.9
The Location for Database, Log Files, and SYSVOL page.

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.

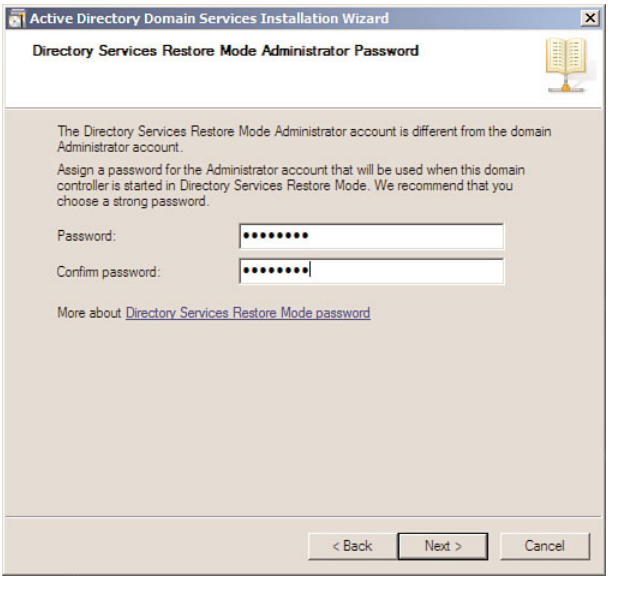


FIGURE 3.10
The Directory Services Restore Mode Administrator Password page.

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.

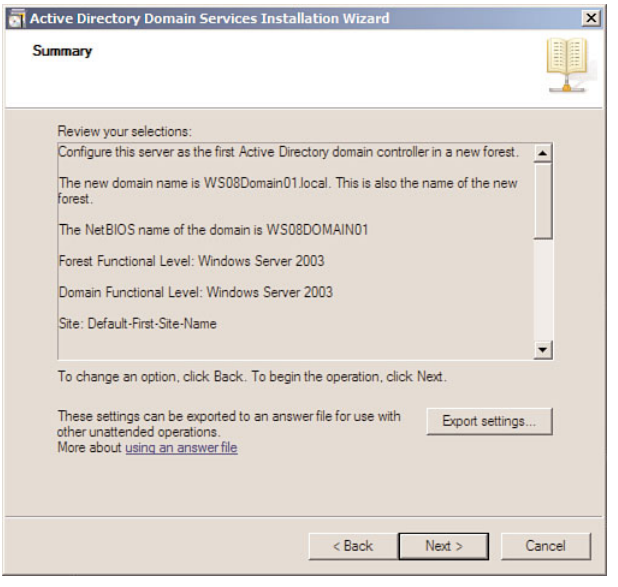


FIGURE 3.11
The Summary page.

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

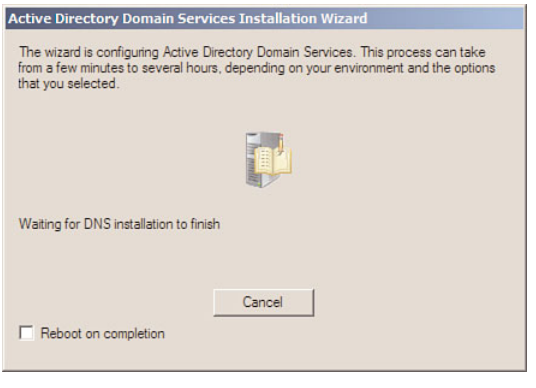


FIGURE 3.12
The Active Directory Domain Services Installation page.

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
`InstallDns:yes`	DNS server will be installed.
`dnsOnNetwork:No`	DNS server will be installed.
`replicaOrNewDomain:domain`	A new domain will be created.
`newDomain:forest`	A new forest will be created.
`newDomainDnsName:WS08Domain02.local`	FQDN of the new domain.
`DomainNetbiosName:WS08Domain02`	NetBIOS name of the new domain.
`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:yes`	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
```

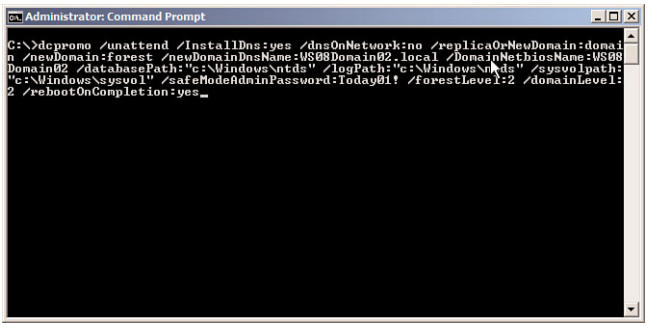


FIGURE 3.14
Installing a new forest using the command line.

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.

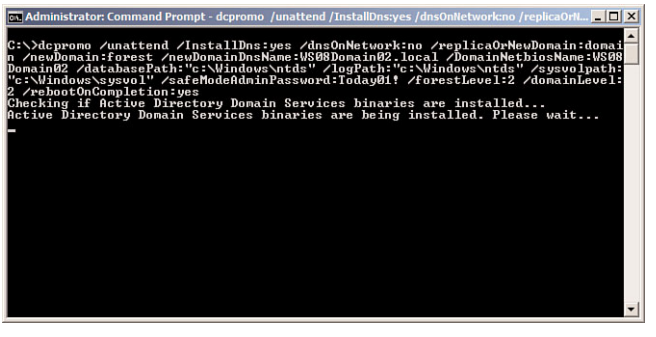


FIGURE 3.15
Installing AD DS services binaries.

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.

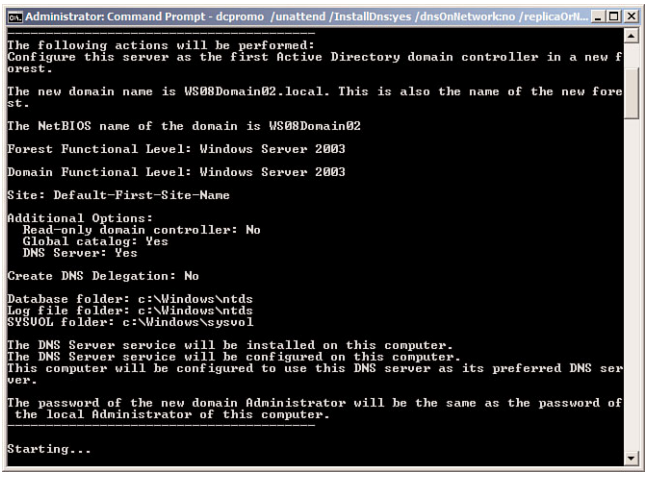


FIGURE 3.16
Installing AD DS.

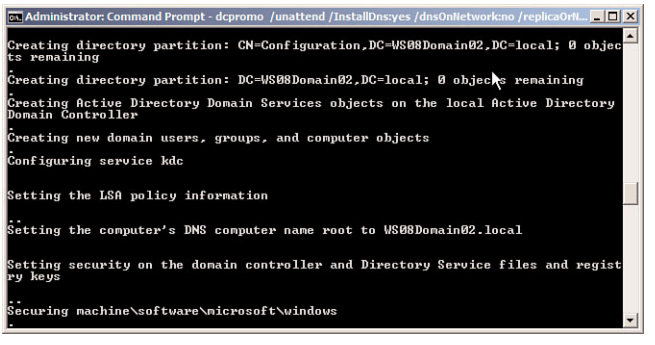


FIGURE 3.17
The installation's progress.

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!
```

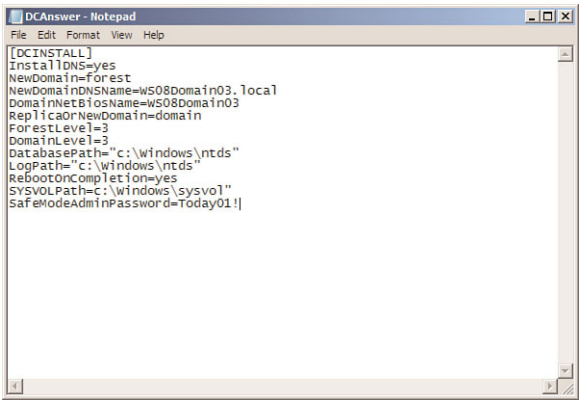


FIGURE 3.18
The answer file.

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.

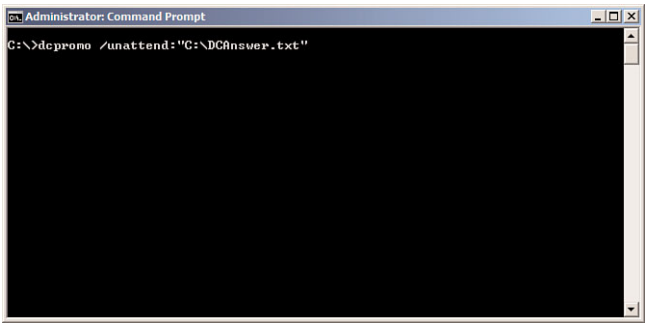


FIGURE 3.19
Installing a new forest by using an answer file.

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.

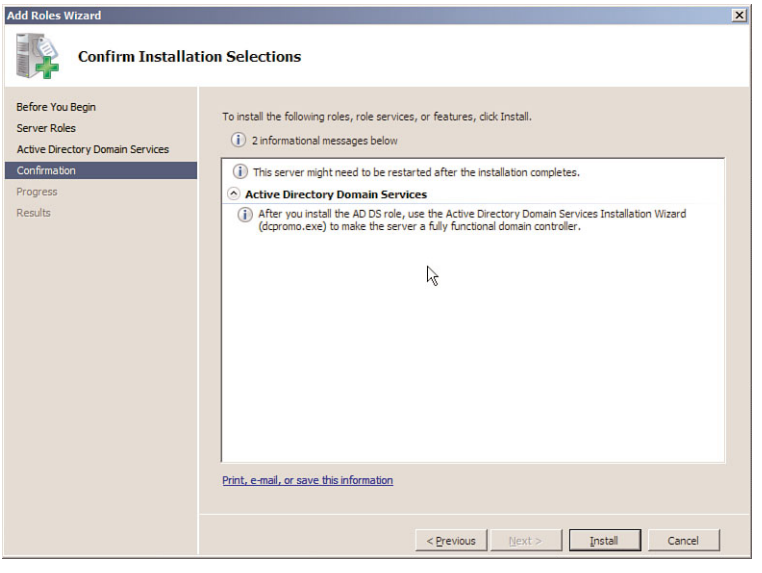


FIGURE 3.20
The Confirm Installation Selections page.

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).

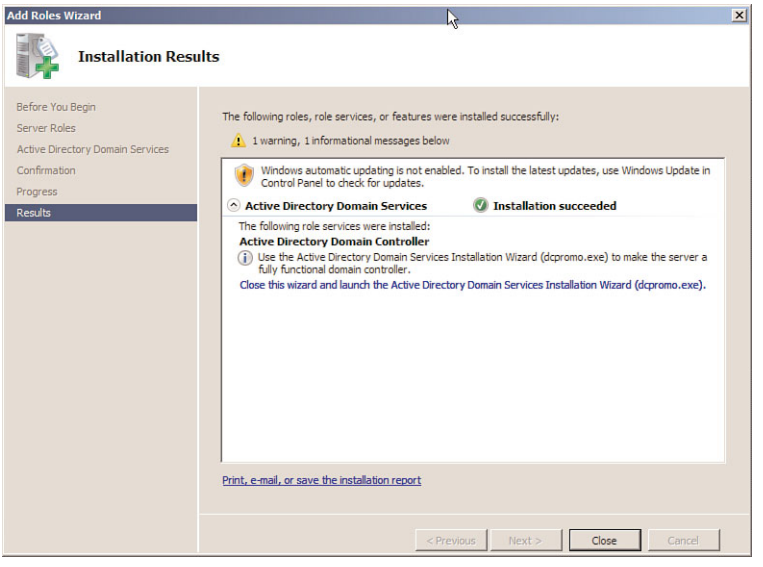


FIGURE 3.21
The Installation Results page.

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.

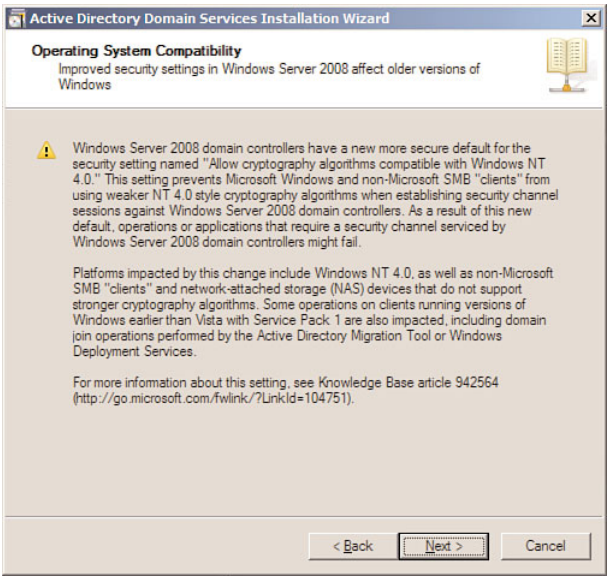


FIGURE 3.23
The Operating System Compatibility page.

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.

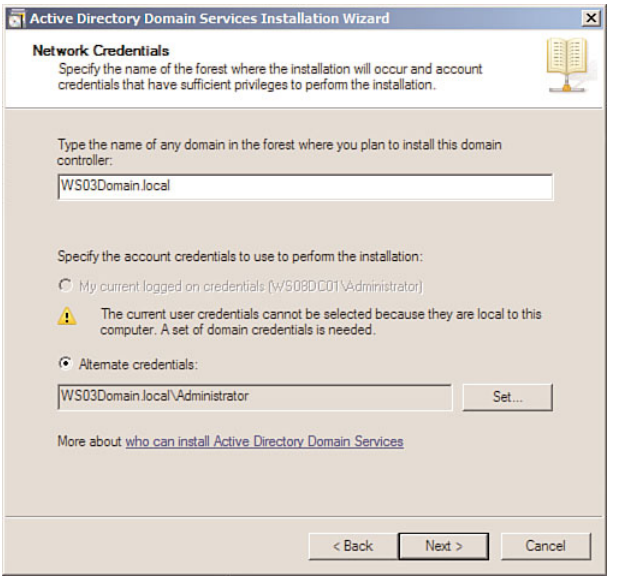


FIGURE 3.24
The Network Credentials page.

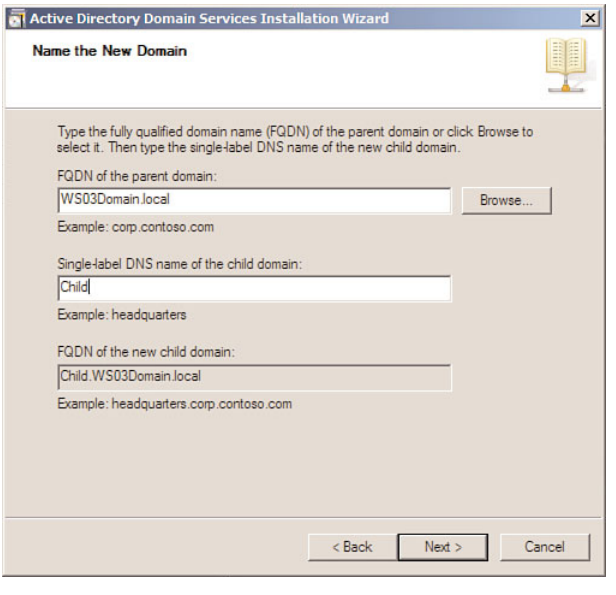


FIGURE 3.25
The Name the New Domain page.

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.

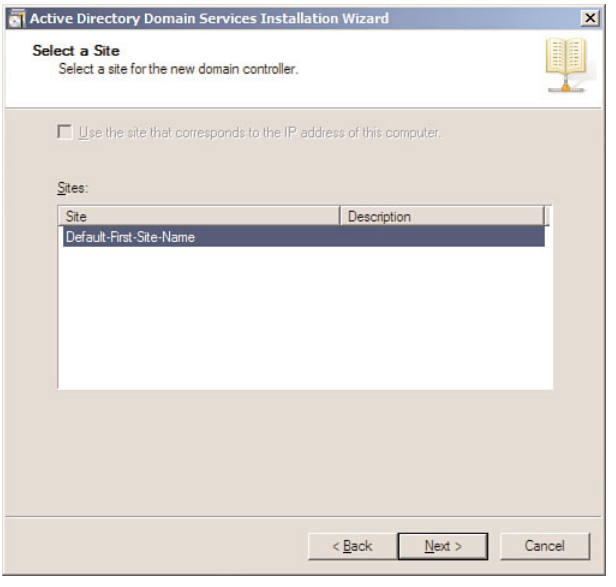


FIGURE 3.26
The Select a Site page.

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.

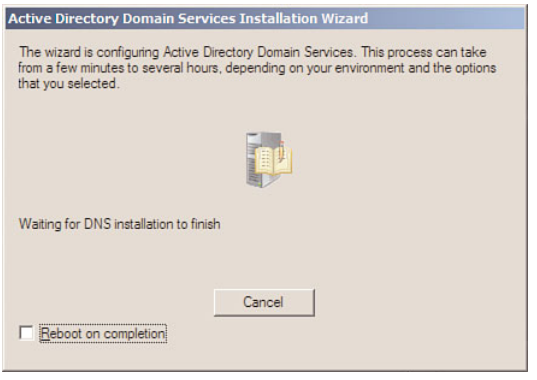


FIGURE 3.27
The Active Directory Domain Services Installation Wizard screen.

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"`	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 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.

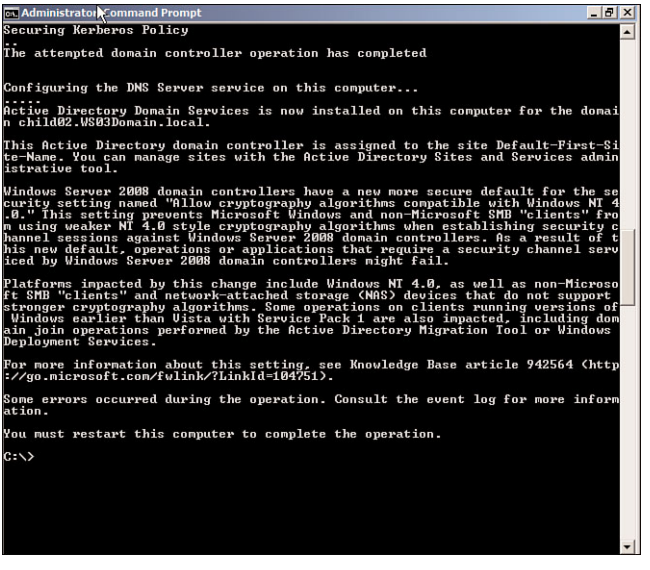


FIGURE 3.28
Installation complete.

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
```

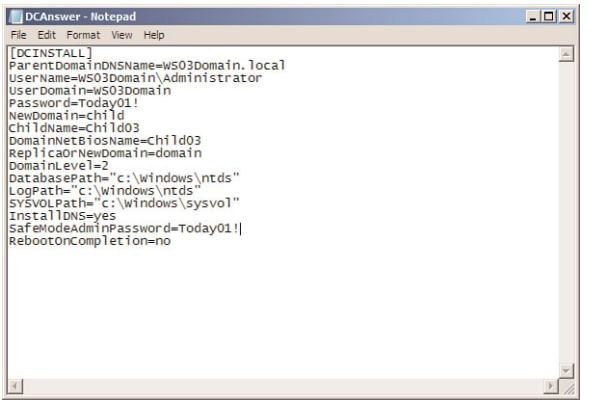


FIGURE 3.29
The answer file.

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.

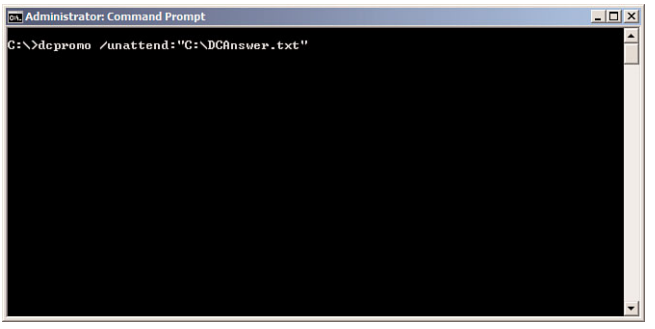


FIGURE 3.30
Installing a new child domain using an answer file.

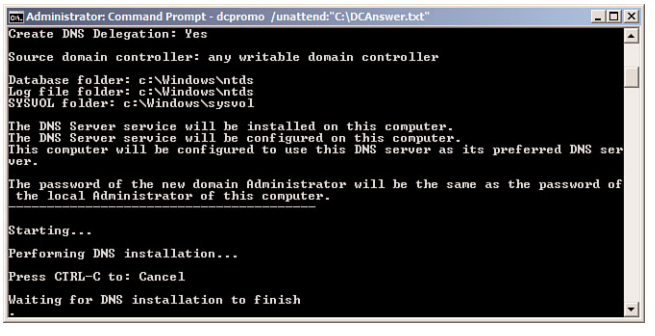


FIGURE 3.31
The status of installing AD DS.

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 **`dcpromo`**, 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 dcpromo 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.

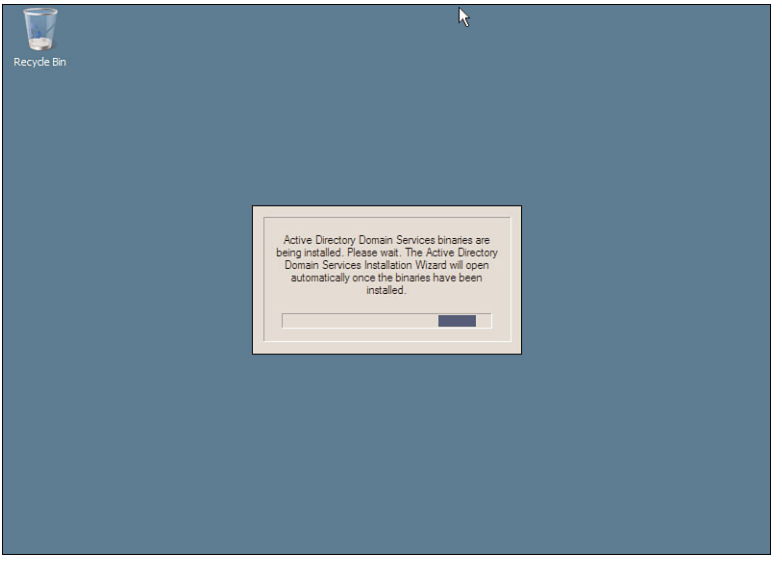


FIGURE 3.32
Installing AD DS server role using dcpromo.

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.

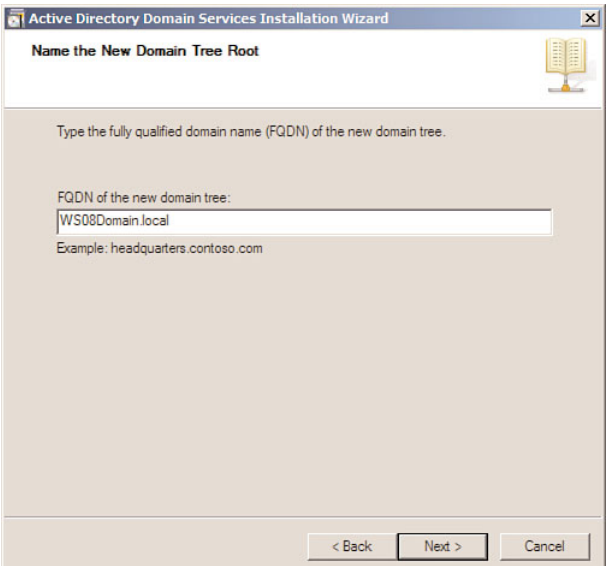


FIGURE 3.33
The Name the New Domain Tree Root page.

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

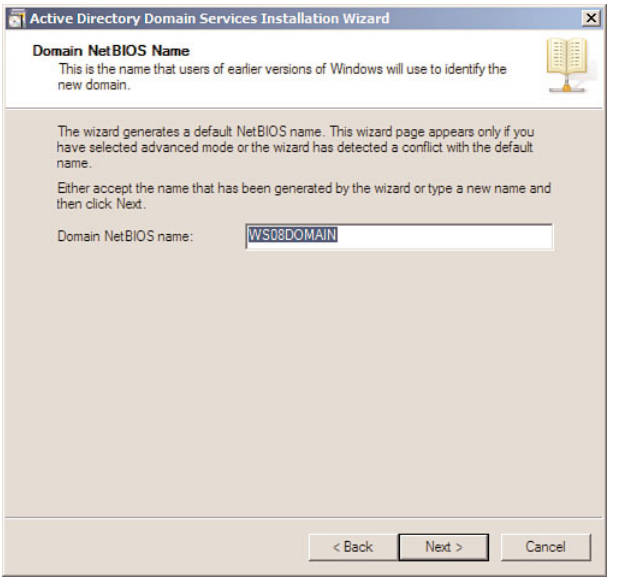


FIGURE 3.34
The Domain NetBIOS Name page.

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.

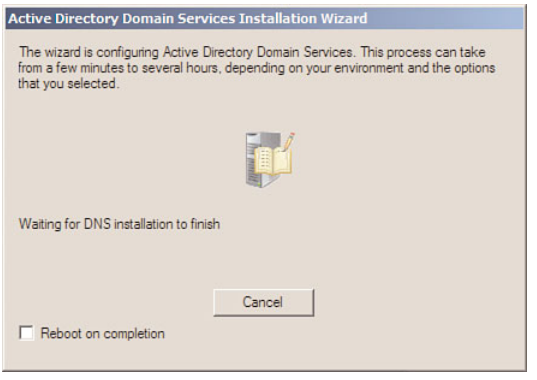


FIGURE 3.35
The Active Directory Domain Services Installation Wizard page.

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!
```

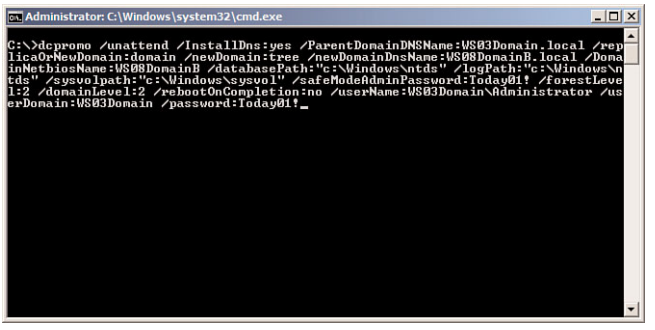


FIGURE 3.36
Installing a new domain tree using the command line.

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"
```

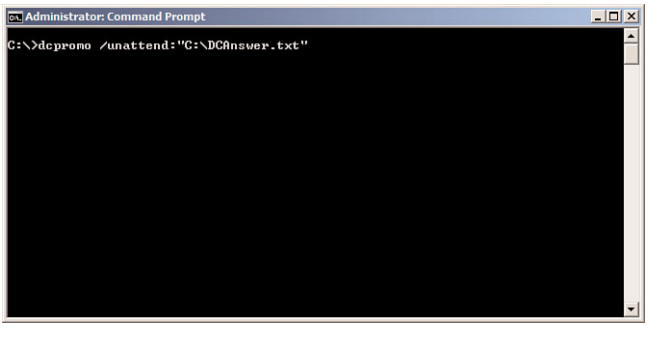


FIGURE 3.37
Installing a domain tree using an answer file.

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.

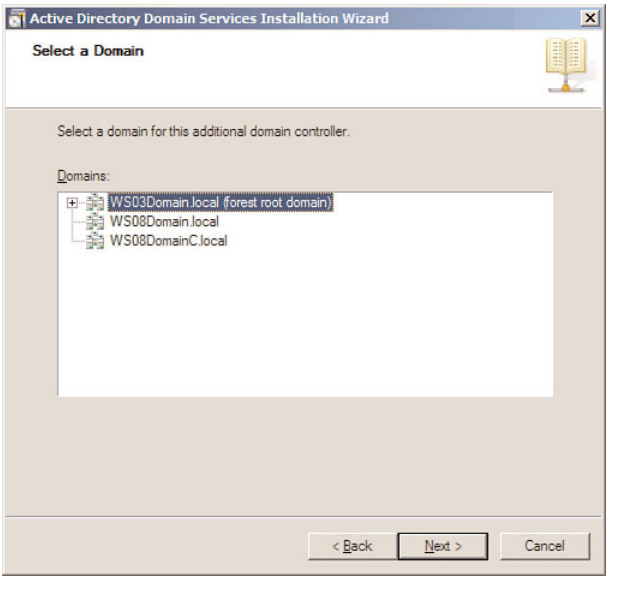


FIGURE 3.38
The Select a Domain page.

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
```

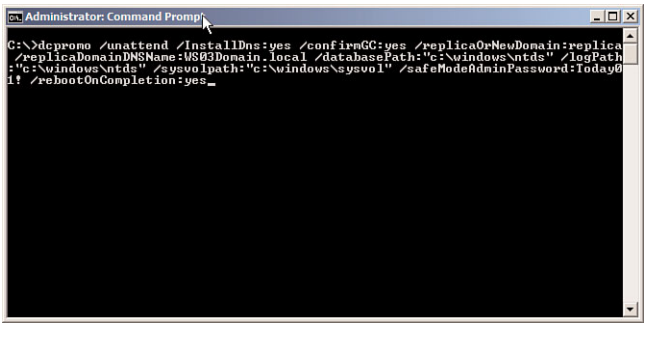


FIGURE 3.39
Installing an additional DC using the command line.

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"
```

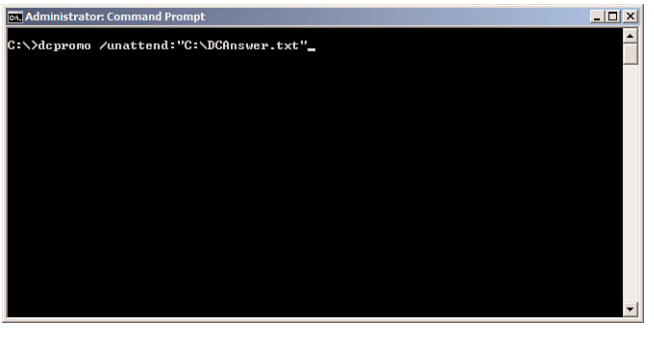


FIGURE 3.40
Installing an additional DC by using an answer file.

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.

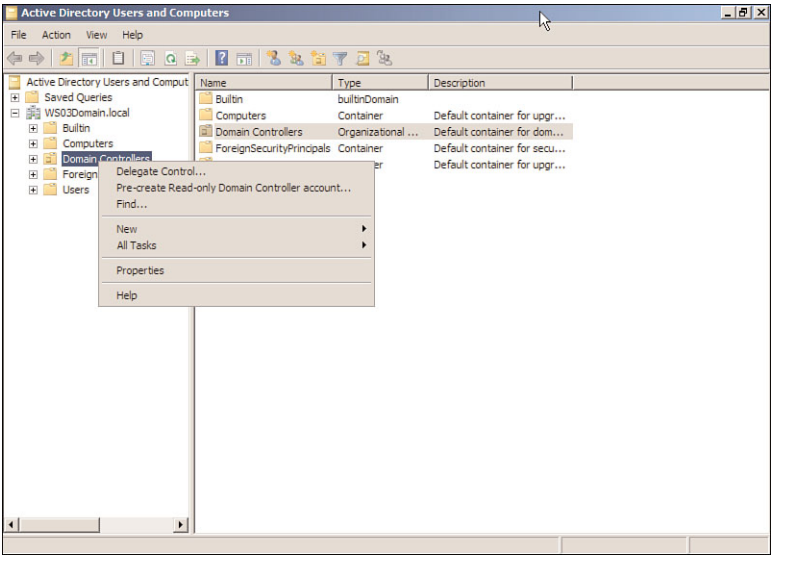


FIGURE 3.41
Selecting Pre-create Read-only Domain Controller account.

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.

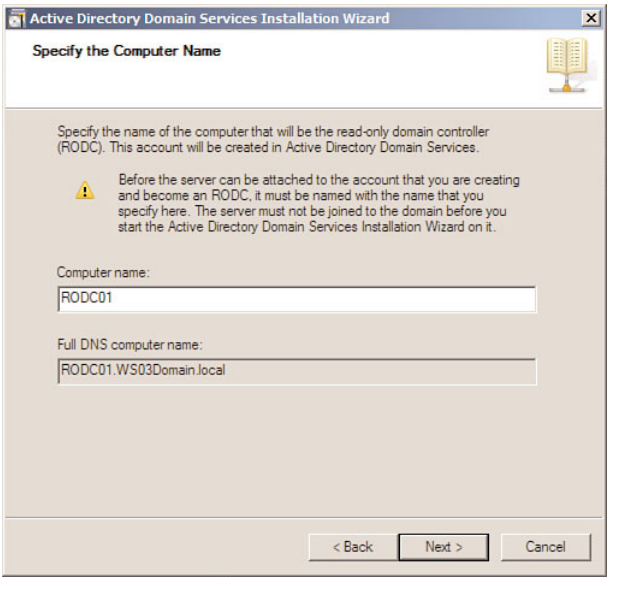


FIGURE 3.43
The Specify the Computer Name page.

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.

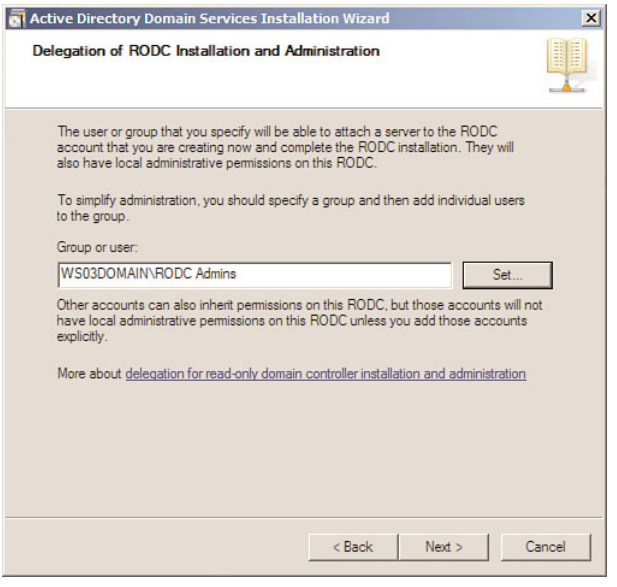


FIGURE 3.44
The Delegation of RODC Installation and Administration page.

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.

6. 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.

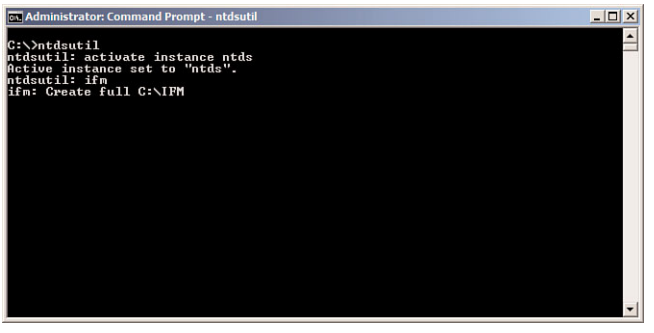


FIGURE 3.45
IFM prompt.

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

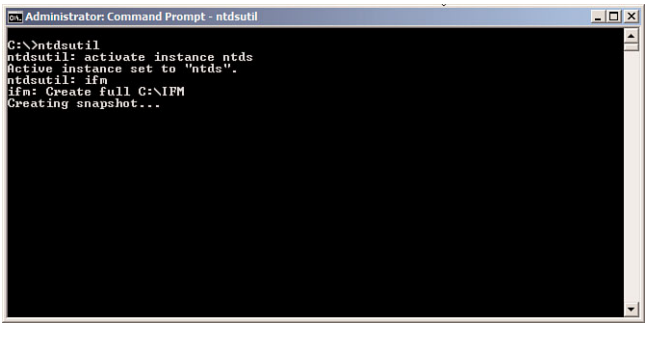


FIGURE 3.46
Create ifm installation media.

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

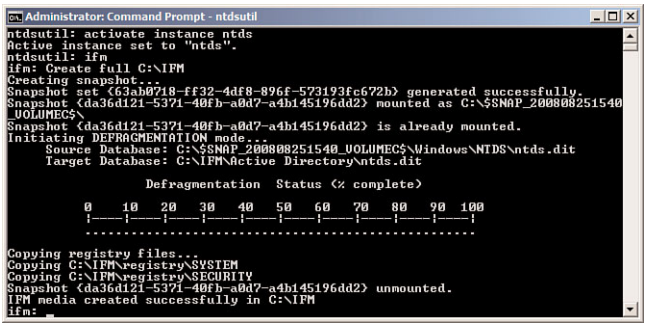


FIGURE 3.47
The IFM created successfully.

9. Type **Q** to exit the `ifm:` prompt.
10. Type **Q** to exit `ntdsutil`.
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.

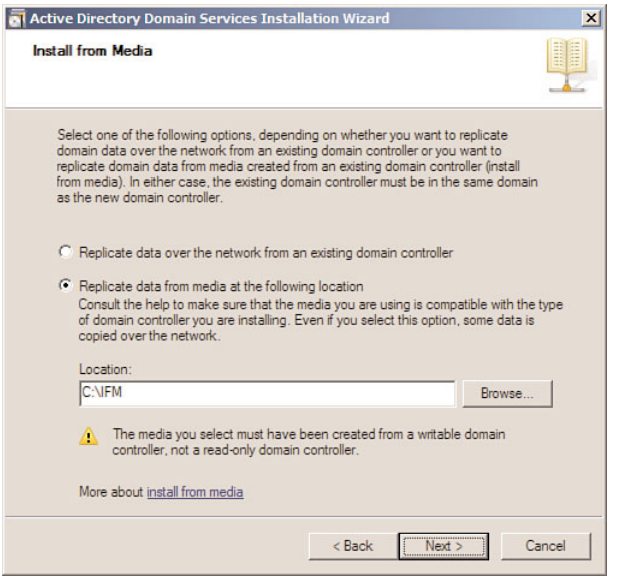


FIGURE 3.48
The Install from Media page.

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.

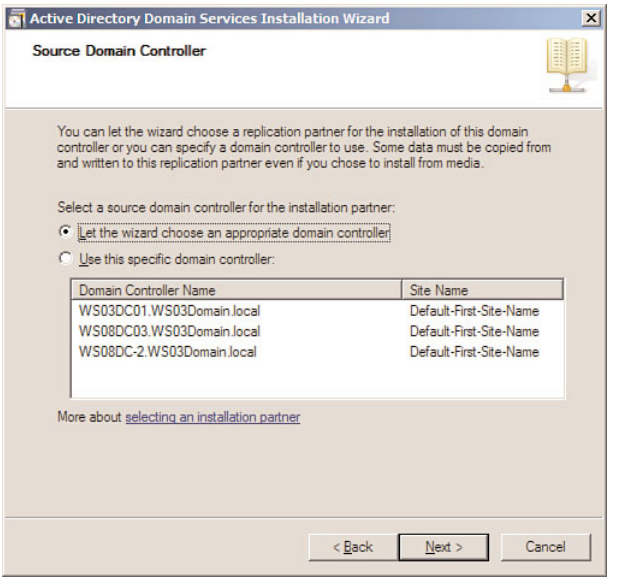


FIGURE 3.49
The Source Domain Controller page.

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.

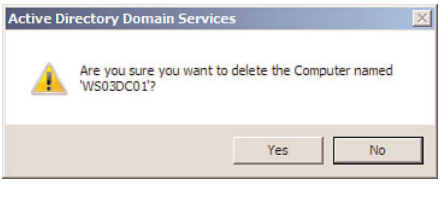


FIGURE 3.51
Confirming computer deletion.

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.

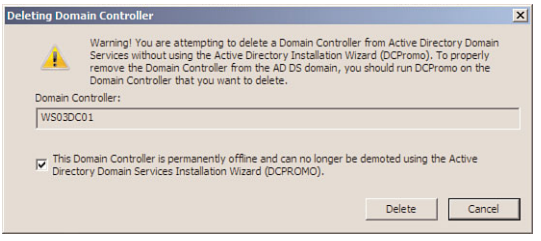


FIGURE 3.55
The Deleting Domain Controller dialog box.

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.

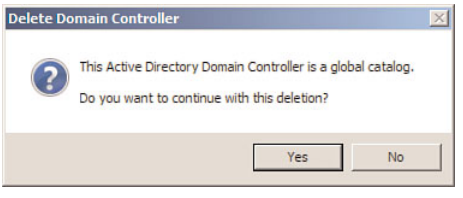


FIGURE 3.56
Global catalog deletion confirmation.

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

B

C

D

E - F

G

H - I

J - K - L

M

N

O

P

Q - R

S

T

U

V - W - X - Y - Z