Active Directory

William R. Stanek
Author and Series Editor

Administrator’s Pocket Consultant
# Contents at a Glance

*Introduction* xv

## PART I IMPLEMENTING ACTIVE DIRECTORY

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Overview of Active Directory</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Installing New Forests, Domain Trees, and Child Domains</td>
<td>29</td>
</tr>
<tr>
<td>3</td>
<td>Deploying Writable Domain Controllers</td>
<td>73</td>
</tr>
<tr>
<td>4</td>
<td>Deploying Read-Only Domain Controllers</td>
<td>105</td>
</tr>
</tbody>
</table>

## PART II MANAGING ACTIVE DIRECTORY INFRASTRUCTURE

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Configuring, Maintaining, and Troubleshooting Global Catalog Servers</td>
<td>139</td>
</tr>
<tr>
<td>6</td>
<td>Configuring, Maintaining, and Troubleshooting Operations Masters</td>
<td>167</td>
</tr>
<tr>
<td>7</td>
<td>Managing Active Directory Sites, Subnets, and Replication</td>
<td>189</td>
</tr>
</tbody>
</table>

## PART III MAINTAINING AND RECOVERING ACTIVE DIRECTORY

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Managing Trusts and Authentication</td>
<td>227</td>
</tr>
<tr>
<td>9</td>
<td>Maintaining and Recovering Active Directory</td>
<td>259</td>
</tr>
<tr>
<td>APPENDIX A</td>
<td>Active Directory Utilities Reference</td>
<td>295</td>
</tr>
</tbody>
</table>

*Index* 321
# Contents

*Introduction xv*

## PART I IMPLEMENTING ACTIVE DIRECTORY

### Chapter 1 Overview of Active Directory 3

- Understanding Directory Services ................................ 3
- Introducing Active Directory ........................................ 5
  - Active Directory Domains ......................................... 5
  - DNS Domains .......................................................... 6
  - Domain Controllers .................................................. 8
- Active Directory Objects ............................................. 11
  - Active Directory Schema ......................................... 12
  - Active Directory Components .................................... 14
- Managing Active Directory .......................................... 22
  - Working with Active Directory ................................... 23
  - Active Directory Administration Tools ......................... 23

### Chapter 2 Installing New Forests, Domain Trees, and Child Domains 29

- Preparing for Active Directory Installation ..................... 29
- Working with Directory Containers and Partitions .............. 30
- Establishing or Modifying Your Directory Infrastructure ....... 31
- Establishing Functional Levels ..................................... 36
- Deploying Windows Server 2008 .................................... 40
- Creating Forests, Domain Trees, and Child Domains .......... 41
  - Installing the AD DS Binaries ................................... 41
  - Creating New Forests .............................................. 42

---

*What do you think of this book? We want to hear from you!*

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

[microsoft.com/learning/booksurvey](http://microsoft.com/learning/booksurvey)
Creating New Domain Trees 59
Creating New Child Domains 66

Chapter 3  Deploying Writable Domain Controllers 73
Preparing to Deploy or Decommission Domain Controllers . . . . 73
Adding Writable Domain Controllers . . . . . . . . . . . . . . . . . . 74
   Installing Additional Writable Domain Controllers 75
   Adding Writable Domain Controllers Using Replication 76
   Adding Writable Domain Controllers Using Installation Media 83
   Adding Writable Domain Controllers Using Answer Files or the Command Line 85
Decommissioning Domain Controllers . . . . . . . . . . . . . . . . . 88
   Preparing to Remove Domain Controllers 88
   Removing Additional Domain Controllers 90
   Removing the Last Domain Controller 94
   Removing Domain Controllers Using Answer Files or the Command Line 95
Forcing the Removal of Domain Controllers . . . . . . . . . . . . . 97
   Restarting a Domain Controller in Directory Services Restore Mode 97
   Performing Forced Removal of Domain Controllers 99
   Cleaning Up Metadata in the Active Directory Forest 102

Chapter 4  Deploying Read-Only Domain Controllers 105
Preparing to Deploy Read-Only Domain Controllers . . . . . . . . . 106
Adding RODCs to Domains . . . . . . . . . . . . . . . . . . . . . . . . . 108
   Adding RODCs Using Replication 109
   Adding RODCs Using Answer Files or the Command Line 115
Using Staged Installations . . . . . . . . . . . . . . . . . . . . . . . . 119
   Stage 1: Creating the RODC Account and Preparing for Installation 120
   Stage 2: Attaching the RODC and Finalizing Installation 121
Performing Staged Installations Using the Command Line or Answer Files | 123
Decommissioning RODCs ................................ | 126
Setting Password Replication Policy ................. | 127
  Password Replication Policy Essentials | 127
  Allowing and Denying Accounts | 130
  Managing Credentials on RODCs | 132
  Identifying Allowed or Denied Accounts | 133
  Resetting Credentials | 134
  Delegating Administrative Permissions | 135

**PART II MANAGING ACTIVE DIRECTORY INFRASTRUCTURE**

**Chapter 5 Configuring, Maintaining, and Troubleshooting Global Catalog Servers** | 139
  Working with Global Catalog Servers ................ | 140
  Deploying Global Catalog Servers ................... | 141
    Adding Global Catalog Servers | 141
    Monitoring and Verifying Global Catalog Promotion | 143
    Identifying Global Catalog Servers | 149
    Restoring Global Catalog Servers | 150
    Removing Global Catalog Servers | 151
    Controlling SRV Record Registration | 152
  Managing and Maintaining Universal Group Membership Caching ................ | 152
    Universal Group Membership Caching Essentials | 152
    Enabling Universal Group Membership Caching | 153
    Monitoring and Troubleshooting Universal Group Membership Caching | 155
  Managing and Maintaining Replication Attributes .......... | 158
    Understanding Global Catalog Search and the Partial Attribute Set | 158
    Designating Replication Attributes | 159
    Monitoring and Troubleshooting Replication Attributes | 163
Managing and Maintaining Name Suffixes ....................... 163
Configuring User Principal Name Suffixes 164
Configuring Name Suffix Routing 165

Chapter 6 Configuring, Maintaining, and Troubleshooting Operations Masters 167
Operations Master Essentials ................................. 167
Introducing Operations Masters 168
Identifying Operations Masters 169
Planning for Operations Masters 169
Changing Operations Masters 170
Working with Operations Masters ......................... 171
Managing Domain Naming Masters 172
Managing Infrastructure Masters 173
Managing PDC Emulators 175
Managing Relative ID Masters 177
Managing Schema Masters 180
Maintaining Operations Masters ...................... 181
Preparing Standby Operations Masters 181
Decommissioning Operations Masters 183
Reducing Operations Master Workload 183
Seizing Operations Master Roles 185
Troubleshooting Operations Masters 187

Chapter 7 Managing Active Directory Sites, Subnets, and Replication 189
Implementing Sites and Subnets ............................. 189
Working with Sites 190
Setting Site Boundaries 190
Replication Essentials ........................................ 191
The Replication Model 191
Replication with Multiple Sites 192
SYSVOL Replication 193
Essential Services for Replication 193
Intrasite Versus Intersite Replication .......................... 194  
Intrasite Replication 194  
Intersite Replication 195  
Developing Your Site Design ................................. 197  
Mapping Your Network Structure 197  
Designing Your Sites 198  
Designing Your Intersite Replication Topology 198  
Configuring Sites and Subnets .............................. 200  
Creating Sites 200  
Creating Subnets 202  
Adding Domain Controllers to Sites 203  
Ensuring Clients Find Domain Controllers 205  
Configuring Site Links and Intersite Replication ............ 206  
Understanding Site Links 206  
Creating Site Links 208  
Configuring Link Replication Schedules 210  
Bridging Sites 212  
Locating and Designating Bridgehead Servers 213  
Locating ISTGs 216  
Optimizing Site Link Configurations 217  
Monitoring, Verifying, and Troubleshooting Replication ...... 218  
Monitoring Replication 218  
Troubleshooting Replication 219  
Generating Replication Topology 222  
Verifying and Forcing Replication 222  

PART III MAINTAINING AND RECOVERING ACTIVE DIRECTORY  

Chapter 8 Managing Trusts and Authentication 227  
Active Directory Authentication and Trusts .................. 227  
Trust Essentials 227  
Authentication Essentials 229  
Authentication Across Domain Boundaries 232  
Authentication Across Forest Boundaries 232
## Working with Domain and Forest Trusts
- Examining Trusts
- Establishing Trusts
- Creating External Trusts
- Creating Shortcut Trusts
- Creating Forest Trusts
- Creating Realm Trusts
- Removing Manually Created Trusts
- Verifying and Troubleshooting Trusts

## Configuring Selective Authentication
- Enabling or Disabling Selective Authentication for External Trusts
- Enabling or Disabling Selective Authentication for Forest Trusts
- Granting the Allowed To Authenticate Permission

## Chapter 9: Maintaining and Recovering Active Directory

### Protecting Objects from Accidental Deletion

### Starting and Stopping Active Directory Domain Services

### Setting the Functional Level of Domains and Forests

### Configuring Deleted Item Retention

### Configuring the Windows Time Service
- Understanding Windows Time
- Working with W32tm
- Checking the Windows Time Configuration
- Configuring an Authoritative Time Source
- Troubleshooting Windows Time Services
- Configuring Windows Time Settings in Group Policy

### Backing Up and Recovering Active Directory
- Active Directory Backup and Recovery Essentials
- Backing Up and Restoring the System State
- Performing a Nonauthoritative Restore of Active Directory
- Performing an Authoritative Restore of Active Directory
Acknowledgments

You know you’ve been at this thing called writing a long time when people ask how many books you’ve written and you just have no idea. For many years, my bio stated that I was the author of more than 25 books. Several times my publishers have asked me to update the bio with a more precise number, so around number 61 I started counting to keep everyone happy. That was about five, six, seven years ago, so I’m now getting close to 100 or thereabouts. ;-)  

For me, it’s always been about the craft of writing. I love writing, and I love challenging projects most of all. The challenge in writing a day-to-day administrator’s guide to Active Directory is that there’s so much I’d like to cover, but pocket consultants aren’t meant to be all-in-one references. Pocket consultants are meant to be portable and readable—the kind of book you use to solve problems and get the job done wherever you might be. With that in mind, I have to continually make sure I focus on the core of Active Directory administration. The result is the book you hold in your hand, which I hope you’ll agree is one of the best practical, portable guides to Active Directory.

As I’ve stated in the three dozen or so pocket consultants I’ve written, the team at Microsoft Press is topnotch. Maria Gargiulo was instrumental throughout the writing process. She helped ensure that I had what I needed to write the book and was my primary contact at Microsoft. Martin DelRe was the acquisitions editor for the project. He believed in the book from the beginning and was really great to work with. Completing and publishing the book wouldn’t have been possible without their help!  

Unfortunately for the writer (but fortunately for readers), writing is only one part of the publishing process. Next came editing and author review. I must say, Microsoft Press has the most thorough editorial and technical review process I’ve seen anywhere—and I’ve written a lot of books for many different publishers. John Pierce managed the editorial process. He helped me stay on track and on schedule. Randy Muller was the technical editor for the book. As copyeditor, Shannon Leavitt also did a good job. Thank you so much!  

I would like to thank Chris Nelson for his help during this project. Chris is terrific to work with and always willing to help any way he can. Thanks also to everyone else at Microsoft who has helped at many points of my writing career and been there when I needed them the most.

Thanks also to Studio B, The Salkind Agency, and my agent Neil Salkind.

Hopefully, I haven’t forgotten anyone, but if I have, it was an oversight. Honest. ;-}
Active Directory Administrator’s Pocket Consultant is designed to be a concise and compulsively usable resource for Windows administrators. This is the readable resource guide you’ll want on your desk or in your pocket at all times. The book discusses everything you need to perform the core administrative tasks for Active Directory. Because the focus is on providing you with the maximum value in a pocket-sized guide, you don’t have to wade through hundreds of pages of extraneous information to find what you’re looking for. Instead, you’ll find exactly what you need to get the job done.

In short, the book is designed to be the one resource you consult whenever you have questions regarding Active Directory administration. To this end, the book concentrates on daily administration procedures, frequently performed tasks, documented examples, and options that are representative but not necessarily inclusive. One of the goals is to keep the content so concise that the book remains compact and easy to navigate while ensuring that the book is packed with as much information as possible—making it a valuable resource. Thus, instead of a hefty thousand-page tome or a lightweight hundred-page quick reference, you get a valuable resource guide that can help you efficiently perform common tasks, solve problems, and implement such advanced administration areas as establishing cross-forest trusts, optimizing intersite replication, changing domain design, and troubleshooting.

Who Is This Book For?

Active Directory Administrator’s Pocket Consultant covers Active Directory for small, medium, and large organizations. The book is designed for:

- Current Windows and network administrators
- Support staff who maintain Windows networks
- Accomplished users who have some administrator responsibilities
- Administrators transferring from other platforms

To pack in as much information as possible, I had to assume that you have basic networking skills and a basic understanding of Windows, and that Windows is already installed on your systems. With this in mind, I don’t devote entire chapters to understanding Windows architecture, installing Windows, or Windows networking. I do, however, provide complete details on the components of Active Directory networks and how you can use these components. I cover installing domain controllers, configuring Active Directory sites, and much more.
I also assume that you are fairly familiar with Windows commands and procedures as well as the Windows user interface. If you need help learning Windows basics, you should read the Windows documentation.

How Is This Book Organized?

Active Directory Administrator's Pocket Consultant is designed to be used in the daily administration of Active Directory, and as such, the book is organized by job-related tasks rather than by features. Speed and ease of reference are essential parts of this hands-on guide. The book has an expanded table of contents and an extensive index for finding answers to problems quickly. Many other quick-reference features have been added as well. These features include quick step-by-step instructions, lists, tables with fast facts, and extensive cross-references. The book is organized into both parts and chapters.

Active Directory is an extensible directory service that enables you to manage network resources efficiently. Part I, “Implementing Active Directory,” reviews the fundamental tasks you need for Active Directory administration. Chapter 1 provides an overview of tools, techniques, and concepts related to Active Directory. Chapter 2 discusses installing forests, domain trees, and child domains. Updates to Active Directory for Windows Server 2008 Release 2 (R2) are discussed in Chapter 1 and Chapter 2 as well. Chapter 3 details techniques for deploying writable domain controllers and the tasks you’ll need to perform to set up domain controllers. Chapter 4 covers the deployment of read-only domain controllers. Together, these chapters provide the detailed information you need to configure domains and forests, whether you are deploying Active Directory Domain Services for the first time or extending your existing infrastructure.

Part II, “Managing Active Directory Infrastructure,” discusses the core tools and techniques you’ll use to manage Active Directory. In addition to their standard roles, domain controllers can also act as global catalog servers and operations masters. Chapter 5 explores techniques for configuring, maintaining, and troubleshooting global catalog servers. Chapter 6 examines how you manage operations masters. Chapter 7 describes your work with Active Directory sites, subnets, and replication. You’ll learn the essentials for creating sites and associating subnets with sites. You’ll also learn advanced techniques for managing site links and replication.

Part III, “Maintaining and Recovering Active Directory,” discusses the administrative tasks you’ll use to maintain Active Directory. Chapter 8 describes how to manage trusts and authentication. You’ll learn how Active Directory authentication works within domains, across domain boundaries, and across forest boundaries. You’ll also learn how trusts are used and established. Chapter 9 provides techniques you can use to maintain, monitor, and troubleshoot Active Directory infrastructure. In addition to learning techniques for backing up and recovering Active Directory, you’ll also learn how to perform essential maintenance tasks and how to configure related options and services, including Windows Time service.
Finally, Appendix A provides a quick reference for command-line utilities you’ll use when working with Active Directory.

**Conventions Used in This Book**

I’ve used a variety of elements to help keep the text clear and easy to follow. You’ll find code terms and listings in monospace type, except when I tell you to actually type a command. In that case, the command appears in **bold** type. When I introduce and define a new term, I put it in *italics*.

Other conventions include:

- **Notes**  To provide details on a point that needs emphasis
- **Best Practices**  To examine the best technique to use when working with advanced configuration and administration concepts
- **Cautions**  To warn you of potential problems you should look out for
- **Real World**  To provide real-world advice for advanced topics
- **Security Alerts**  To point out important security issues
- **Tips**  To offer helpful hints or additional information

I truly hope you find that *Active Directory Administrator’s Pocket Consultant* provides everything you need to perform essential Active Directory administrative tasks as quickly and efficiently as possible. You’re welcome to send your thoughts to me at williamstanek@aol.com. Thank you.

**Find Additional Content Online**

As new or updated material becomes available that complements your book, it will be posted online on the Microsoft Press Online Windows Server and Client Web site. The type of material you might find includes updates to book content, articles, links to companion content, errata, sample chapters, and more. This Web site is available at [www.microsoft.com/learning/books/online/serverclient](http://www.microsoft.com/learning/books/online/serverclient) and is updated periodically.

**Support**

Every effort has been made to ensure the accuracy of this book. Microsoft Press provides corrections for books through the World Wide Web at the following address:

[http://www.microsoft.com/mspress/support](http://www.microsoft.com/mspress/support)
If you have comments, questions, or ideas about this book, please send them to Microsoft Press, using either of the following methods:

Postal mail:
Microsoft Press
Attn: Editor, Active Directory Administrator’s Pocket Consultant
One Microsoft Way
Redmond, WA 98052-6399

E-mail:
mspinput@microsoft.com

Please note that product support isn’t offered through these addresses. For support information, visit Microsoft’s Web site at http://support.microsoft.com.
Preparing to Deploy or Decommission Domain Controllers

Before deploying or decommissioning domain controllers, you should create a plan that lists any prerequisites, necessary postmodification changes, and overall impact on your network. Create your plan by reviewing “Preparing for Active Directory Installation” in Chapter 2, “Installing New Forests, Domain Trees, and Child Domains.”

Domain controllers host the Active Directory database and handle related operations. Active Directory uses a multimaster replication model that creates a distributed environment where no single domain controller is authoritative with regard to logon and authentication requests. This model allows any domain controller to be used for logon and authentication. It also allows you to make changes to standard directory information without regard to which domain controller you use.
Domain controllers also can have special roles as operations masters and global catalog servers. As discussed in Chapter 5, “Managing Operations Masters,” operations masters perform tasks that can be performed only by a single authoritative domain controller. Global catalog servers store partial replicas of data from all domains in a forest to facilitate directory searches for resources in other domains and to determine membership in universal groups.

When you establish the first domain controller in a forest, the domain controller hosts the forestwide and domainwide operations master roles and also acts as the global catalog server for the domain. When you establish the first domain controller in a domain, the domain controller hosts the domainwide operations master roles and also acts as the global catalog server for the domain.

Every domain in the enterprise should have at least two domain controllers. If a domain has only one domain controller, you could lose the entire domain and all related accounts if disaster strikes. Although you may be able to recover the domain from a backup, you will have significant problems until the restore is completed. For example, users may not be able to log on to the domain or obtain authenticated access to domain resources.

Every site should have at least one domain controller. If a domain controller is not available in a site, computers in the site will perform logon and authentication activities with domain controllers in another site, which could significantly affect response times.

Every site should have a global catalog server. If a global catalog server is not available in a site, computers in the site will query a global catalog server in another site when searching for resources in other domains in the forest. Global catalog servers are also used during logon and authentication because they store universal group membership information for all domains in the forest. If a global catalog server isn’t available in the site and the universal group membership has not been previously cached, the domain controller responding to a user’s logon or authentication request will need to obtain the required information from a global catalog server in another site.

**Adding Writable Domain Controllers**

You establish a server as a domain controller by installing the necessary binaries for the Active Directory Domain Services (AD DS) and then configuring the services using the Active Directory Domain Services Installation Wizard (Dcpromo.exe). If you are deploying Windows Server 2008 for the first time in a Windows Server 2003 or Windows Server 2000 forest, you must prepare Active Directory as discussed in “Deploying Windows Server 2008” in Chapter 2.
Installing Additional Writable Domain Controllers

Any computer running Windows Server 2008 can act as a domain controller. Essentially, domain controllers are database servers with extensive directory, application, and replication features. Because of this, the hardware you choose for the domain controllers should be fairly robust. You’ll want to look carefully at the server’s processor, memory, and hard disk configuration.

In many cases, you’ll want to install domain controllers on hardware with multiple, fast processors. This will help ensure the domain controller can efficiently handle replication requests and topology generation. When you install the second domain controller in a forest, the Knowledge Consistency Checker (KCC) begins running on every domain controller. Not only does the KCC generate replication topology, it also dynamically handles changes and failures within the topology. By default, the KCC recalculates the replication topology every 15 minutes. As the complexity of the replication topology increases, so does processing power required for this calculation. You’ll need to monitor processor usage and upgrade as necessary.

In addition to running standard processes, domain controllers must run processes related to storage engine operations, knowledge consistency checking, replication, and garbage collection. Most domain controllers should have at least 2 gigabytes (GB) of RAM as a recommended starting point for full server installations and 1 GB of RAM for core server installations. You’ll need to monitor memory usage and upgrade as necessary.

With regard to hard disks, you’ll want to closely examine fault tolerance and storage capacity needs. Domain controllers should use fault-tolerant drives to protect against hardware failure of the system volume and any other volumes used by Active Directory. I recommend using a redundant array of independent disks (RAID), RAID 1 for system volumes and RAID 5 for data. Hardware RAID is preferable to software RAID. Storage capacity needs depend on the number of objects related to users, computers, groups, and resources that are stored in the Active Directory database. Each storage volume should have ample free disk space at all times to ensure proper operational efficiency.

When you add a domain controller to an existing domain, you should consider whether you want to perform an installation from media rather than creating the domain controller from scratch. With either technique, you will need to log on to the local machine using either the local Administrator account or an account that has administrator privileges on the local machine. Then start the installation. You also will be required to provide the credentials for an account that is a member of the Domain Admins group in the domain of which the domain controller will be a part. Because you will be given the opportunity to join the domain controller to the domain if necessary, it is not necessary for the server to be a member of the domain.
Adding Writable Domain Controllers Using Replication

You can add a writable domain controller to an existing domain by completing the following steps:

1. Check the TCP/IP configuration of the server. The server must have a valid IP address and must have properly configured DNS settings.
   
   **NOTE** Domain controllers that also act as DNS servers should not have dynamic IP addresses, to ensure reliable DNS operations. Otherwise, the server can have a static IP address or a dynamic IP address assigned by a DHCP server.

2. Install the Active Directory binaries by entering the following command at an elevated command prompt: `servermanagercmd –install adds-domain-controller`. This installs the AD DS binaries, which enables the Active Directory Domain Services role on the server.

3. Before starting an Active Directory installation, you should examine local accounts to determine whether you need to take special steps to preserve any local accounts. You should also check for encrypted files and folders using the EFSInfo utility. At a command prompt, enter `efsinf /s:DriveDesignator /i | find “: Encrypted”` where DriveDesignator is the drive designator of the volume to search, such as C:
   
   **CAUTION** Domain controllers do not have local accounts or separate cryptographic keys. Making a server a domain controller deletes all local accounts and all certificates and cryptographic keys from the server. Any encrypted data on the server, including data stored using the Encrypting File System (EFS), must be decrypted before Active Directory is installed, or it will be permanently inaccessible.

4. Start the Active Directory Domain Services Installation Wizard by clicking Start, typing `dcpromo` in the Search box, and pressing Enter.

5. By default, the wizard uses Basic Installation mode. If you want to install from media as discussed in “Adding Writable Domain Controllers Using Installation Media,” later in this chapter, or choose the source domain controller for replication, select the Use Advanced Installation Mode check box before clicking Next to continue.

6. If the Operating System Compatibility page is displayed, review the warning about the default security settings for Windows Server 2008 domain controllers and then click Next.

7. On the Choose A Deployment Configuration page, shown in Figure 3-1, select Existing Forest and then select Add A Domain Controller To An Existing Domain. By choosing this option, you specify that you are adding a domain controller to an existing domain in the Active Directory forest.
Specify that you want to add a domain controller to the domain.

8. When you click Next, you see the Network Credentials page, shown in Figure 3-2. In the field provided, type the full DNS name of any domain in the forest where you plan to install the domain controller. Preferably, this should be the name of the forest root domain, such as cpandl.com. If you are logged on to a domain in this forest and have the appropriate permissions, you can use your current logged-on credentials to perform the installation. Otherwise, select Alternate Credentials, click Set, type the user name and password for an enterprise administrator account in the previously specified domain, and then click OK.
9. When you click Next, the wizard validates the domain name you provided and then lists all domains in the related forest. On the Select A Domain page, shown in Figure 3-3, select the domain to which the domain controller will be added and then click Next.

**FIGURE 3-2** Set the network credentials.

**FIGURE 3-3** Select the target domain.
10. When you click Next, the wizard determines the available Active Directory sites. On the Select A Site page, you’ll see a list of available sites. If there is a site that corresponds to the IP address of the server you are promoting, select the Use The Site That Corresponds To The IP Address check box to place the new domain controller in this site. If you want to place the new domain controller in a different site or there isn’t an available subnet for the current IP address, select the site in which you want to locate the domain controller.

11. When you click Next, the wizard examines the DNS configuration and attempts to determine whether any authoritative DNS servers are available. It then displays the Additional Domain Controller Options page, shown in Figure 3-4. As permitted, select additional installation options for the domain controller and then click Next.

![Active Directory Domain Services Installation Wizard](image)

**FIGURE 3-4** Specify the additional installation options.

12. If you choose to let the wizard install the DNS Server service, note the following:

   a. The DNS Server service will be installed, and the domain controller will also act as a DNS server. A primary DNS zone will be created as an Active Directory–integrated zone with the same name as the new domain you are setting up. The wizard will also update the server’s TCP/IP configuration so that its primary DNS server is set to itself.

   b. During installation of the operating system, Windows Setup installs and configures IPv4 and IPv6 if networking components were detected. If
you’ve configured dynamic IPv4, IPv6, or both addresses, you’ll see a warning. Click Yes to ignore the warning and continue.

c. If you want to modify the TCP/IP configuration, click No to return to the Additional Domain Controller Options page and then make the appropriate changes to the system configuration before clicking Next to continue. If you configure a static IPv4 address but do not configure a static IPv6 address, you’ll also see the warning. To ignore the warning and continue with the installation, click Yes.

**NOTE** At a minimum, you should configure a static IPv4 address before continuing. Click Start, type `ncpa.cpl` in the Search box, and then press Enter. In Network Connections, double-click Local Area Connection. In Local Area Connection Properties, click Properties and then double-click Internet Protocol Version 4 (TCP/IPv4), make any necessary changes, and then click OK. If you also want to configure a static IPv6 address, double-click Internet Protocol Version 6 (TCP/IPv6), make any necessary changes, and then click OK. If you decide not to configure a static IPv6 address, you may need to make changes to DNS records later if your organization starts using IPv6 addresses.

d. The wizard next attempts to register a delegation for the DNS server with an authoritative parent zone. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to the DNS server and then click Yes to continue. Otherwise, you can ignore this warning and click Yes to continue.

13. If you choose to not let the wizard install the DNS Server service, the wizard next attempts to register a delegation for the DNS server with an authoritative parent zone. If the wizard cannot create a delegation for the DNS server, it displays a warning message to indicate that you must create the delegation manually. Click No to return to the Additional Domain Controller Options page so you can select and install DNS Server services. To continue without installing DNS Server services, click Yes. Keep in mind that you’ll then need to manually configure the required DNS settings, including SRV and A resource records.

14. If you selected Use Advanced Installation Mode, the Install From Media page is displayed, as shown in Figure 3-5. You can provide the location of installation media to be used to create the domain controller and configure AD DS, or you can have all of the replication done over the network. Even if you install from media, some data will be replicated over the network from a source domain controller. For more information about installing from media, see “Adding Writable Domain Controllers Using Installation Media.”
Deploying Writable Domain Controllers

CHAPTER 3

15. If you selected Use Advanced Installation Mode, the Source Domain Controller page is displayed. Select Any Writable Domain Controller or select This Specific Domain Controller to specify a source domain controller for replication. Then click Next. If you choose to install from media, only changes since the media was created will be replicated from this source domain controller. If you choose not to install from media, all data will be replicated from this source domain controller.

On the Location For Database, Log Files, And SYSVOL page, shown in Figure 3-6, select a location to store the Active Directory database folder, log folder, and SYSVOL folder. The default location for the database and log folders is a subfolder of %SystemRoot%\NTDS. The default location for the SYSVOL folder is %SystemRoot%\Sysvol. You’ll get better performance if the database folder and log folder are on two separate volumes, each on a separate disk. Placement of the SYSVOL is less critical, and you can accept the default in most cases. Although you can change the storage locations later, the process is lengthy and complex.

FIGURE 3-5 Set the installation mode.
NOTE   Your organization should have a specific plan in place for sizing the server hardware and designating Active Directory storage locations. You’ll want to ensure the server you use is powerful enough to handle authentication, replication, and other directory duties. The server’s hard disk configuration should be optimized for storage of Active Directory data. Each storage volume should have at least 20 percent free storage space at all times. You may also want to use a redundant array of independent disks (RAID) to protect against disk failure.

17. Click Next. On the Directory Services Restore Mode Administrator Password page, type and confirm the password that should be used when you want to start the computer in Directory Services Restore Mode. Be sure to track this password carefully. This special password is used only in Restore mode and is different from the Administrator account password. The password complexity and length must comply with the domain security policy.

18. Click Next. On the Summary page, review the installation options. If desired, click Export Settings to save these settings to an answer file that you can use to perform unattended installation of other domain controllers. When you click Next again, the wizard will use the options you’ve selected to install and configure Active Directory. This process can take several minutes. If you specified that the DNS Server service should be installed, the server will also be configured as a DNS server at this time.
19. When the wizard finishes configuring Active Directory, click Finish. You are then prompted to restart the computer. Click Restart Now to reboot.

After installing Active Directory, you should verify the installation. Start by examining the installation log, which is stored in the Dcpromo.log file in the %SystemRoot%\Debug folder. The log is very detailed and takes you through every step of the installation process, including the creation of directory partitions and the securing of the Registry for Active Directory.

Next, check the DNS configuration in the DNS console. DNS is updated to add SRV and A records for the server. Because you created a new domain, DNS is updated to include a forward lookup zone for the domain. You may also need to add a reverse lookup zone for the domain.

Check for updates in Active Directory Users and Computers. The Domain Controllers OU should have an account for the domain controller you installed.

**Adding Writable Domain Controllers Using Installation Media**

Performing an Active Directory installation from media allows the Active Directory Domain Services Installation Wizard to get the initial data for the Configuration, Schema, and Domain directory partitions, and optionally the SYSVOL, from the backup media rather than through a full synchronization over the network. In this way, you establish a domain controller using a media backup of another domain controller rather than using replication over the network. Although not designed to be used to restore failed domain controllers, this technique does help you rapidly establish additional domain controllers by reducing the amount of network traffic generated, accelerating the process of installing an additional domain controller, and getting the directory partition data synchronized.

You can use a 32-bit domain controller to generate installation media for a 64-bit domain controller, and vice versa. When installing Active Directory using a media backup, you’ll want to follow these guidelines:

- Use the most recent media backup to reduce the number of updates that must be replicated.
- Use a backup of a domain controller running the same operating system in the same domain in which the new domain controller is being created.
- Copy the backup to a local drive on the server you are configuring. You cannot use backup media from Universal Naming Convention (UNC) paths or mapped drives.
- Don’t use backup media that is older than the tombstone lifetime of the domain. The default value is 60 days. If you try to use backup media older than the tombstone lifetime, the Active Directory installation will fail.
You can create installation media by completing the following steps:

1. Log on to a domain controller. On a writable domain controller, the account you use must be a member of the Administrators, Server Operators, Domain Admins, or Enterprise Admins group. On a read-only domain controller, a delegated user can create the installation media for another read-only domain controller.

2. Click Start, right-click Command Prompt, and then click Run As Administrator to open an elevated command prompt. At the command prompt, type `ntdsutil`. This starts the Directory Services Management tool.

3. At the ntdsutil prompt, type `activate instance ntds`. This sets Active Directory as the directory service instance to work with.

4. Type `ifm` to access the install from media prompt. Then type one of the following commands, where `FolderPath` is the full path to the folder in which to store the Active Directory backup media files:
   - **Create Full `FolderPath`**  Creates a full writable installation media backup of Active Directory. You can use the media to install a writable domain controller or a read-only domain controller.
   - **Create RODC `FolderPath`**  Creates a read-only installation media backup of Active Directory. You can use the media to install a read-only domain controller. The backup media does not contain security credentials, such as passwords.

5. Ntdsutil creates snapshots of Active Directory partitions. When it finishes creating the snapshots, Ntdsutil mounts the snapshots as necessary and then defragments the media backup of the Active Directory database. The progress of the defragmentation is shown by percent complete.

6. Next, Ntdsutil copies registry data related to Active Directory. When it finishes this process, Ntdsutil unmounts any snapshots it was working with. The backup process should complete successfully. If it doesn’t, note and resolve any issues that prevented successful creation of the backup media, such as the target disk running out of space or insufficient permissions to copy to the folder path.

7. Type `quit` at the ifm prompt and then type `quit` at the ntdsutil prompt.

8. Copy the backup media to a local drive on the server for which you are installing Active Directory.

9. On the server you want to make a domain controller, start the Active Directory Domain Services Installation Wizard in Advanced Installation mode. Follow all the same steps you would if you were adding a domain controller to the domain without media. After you select additional domain controller installation options and get past any DNS prompts, you see the Install From Media page. On this page, select Replicate From Media Stored At The Following Location, and then type the location of the backup media files or click Browse to find the backup media files.
10. You can now complete the rest of the installation as discussed in the section titled “Adding Writable Domain Controllers Using Replication” earlier in this chapter. Continue with the rest of the steps and perform the postinstallation checks as well.

**REAL WORLD** Objects that were modified, added, or deleted since the installation media was created must be replicated. If the installation media was created recently, the amount of replication that is required should be considerably less than the amount of replication required otherwise.

The only data that must be fully replicated from another domain controller is the SYSVOL data. Although you can run Ntdsutil with an option to include the SYSVOL folder in the installation media, the SYSVOL folder from the installation media cannot be used because SYSVOL must be absent when the Active Directory Domain Services server role starts on a server running Windows Server 2008.

### Adding Writable Domain Controllers Using Answer Files or the Command Line

On a Full Server or Core Server installation of Windows Server 2008, you can add domain controllers using an unattended installation or the command line. You must be logged on as the Domain Admins group in the domain.

With the unattended method of installation, you must first prepare an answer file that contains the desired configuration values. You can create the required answer file by completing the following steps:

1. Open Notepad or any other text editor.
2. On the first line, type `[DCINSTALL]`, and then press Enter.
3. Type the following entries, one entry on each line.

```plaintext
ReplicaOrNewDomain=Replica
ReplicaDomainDNSName=FQDNOfDCDomain
SiteName=SiteName
InstallDNS=Yes
ConfirmGc=Yes
CreateDNSDelegation=Yes
UserDomain=DomainOfAdminAccount
UserName=AdminAccountInDomainOfDC
Password=*  
ReplicationSourceDC=SourceDCName
DatabasePath="LocalDatabasePath"
LogPath="LocalLogPath"
SYSVOLPath="LocalSysVolPath"
SafeModeAdminPassword=
RebootOnCompletion=Yes
```
NOTE Values you must specify are shown in bold. You can set Password to * if you do not want to include it in the answer file. When you run Dcpromo to initiate the unattended installation, you will be prompted for the password.

TIP SafeModeAdminPassword sets the Directory Services Restore Mode password in the answer file. If you don’t want to include the password, you can omit the password. However, you will need to use the /SafeModeAdminPassword command-line parameter to provide the password later when you run Dcpromo to initiate the unattended installation.

4. If you want to configure the domain controller as a DNS server, add the following command.

   ```
   InstallDNS=yes
   ```

5. If you want to configure the domain controller as a global catalog server, add the following command.

   ```
   ConfirmGC=yes
   ```

6. If you are installing from media, you can refer to the location where you stored the installation media by using the following command.

   ```
   ReplicationSourcePath=FolderPathToMedia
   ```

7. Save the answer file as a .txt file and then copy the file to a location accessible from the server you want to promote.

   The following is a complete example.

   ```
   ; Replica DC promotion
   [DCInstall]
   ReplicaOrNewDomain=Replica
   ReplicaDomainDNSName=cpandl.com
   SiteName=LA-First-Site
   InstallDNS=Yes
   ConfirmGC=Yes
   CreateDNSDelegation=No
   UserDomain=cpandl.com
   UserName=cpandl.com\williams
   Password=*  
   ReplicationSourceDC=CorpServer65.cpandl.com
   DatabasePath="D:\Windows\NTDS"
   LogPath="D:\Windows\NTDS"
   SYSVOLPath="D:\Windows\SYSVOL"
   ```
8. After you create the answer file, you can start the unattended installation by entering the following at a command prompt:

```bash
dcpromo /unattend:"PathToAnswerFile"
```

where `PathToAnswerFile` is the full file path to the answer file, such as `C:\data\newdc.txt`.

At the command line, you can add a domain controller to a domain using the following command.

```bash
```

If you are installing from media, you can refer to the location where you stored the installation media by using the following command.

```bash
/ReplicationSourcePath:FolderPathToMedia
```

When the unattended installation or command-line execution completes, Dcpromo exits with a return code. A return code of 1 to 10 indicates success. A return code of 11 to 100 indicates failure. Note any related error text and take appropriate corrective action as necessary.
Decommissioning Domain Controllers

When you no longer need a domain controller, you can decommission it and remove it from service. Running the Active Directory Domain Services Installation Wizard (Dcpromo.exe) on the domain controller allows you to remove Active Directory Domain Services and demote the domain controller to either a stand-alone server or a member server.

The process for removing an additional domain controller is different from the process for removing the last domain controller. If the domain controller is the last in the domain, it will become a stand-alone server in a workgroup. Otherwise, if other domain controllers remain in the domain, the domain controller will become a member server in the domain.

Preparing to Remove Domain Controllers

Before you demote a domain controller, you should determine the functions and roles the server has in the domains and plan accordingly. With regard to Active Directory Domain Services, the functions and roles to check for are as follows:

Global catalog server

- Don’t accidentally remove the last global catalog server from a domain. If you remove the last global catalog server from a domain, you will cause serious problems. Users won’t be able to log on to the domain, and directory search functions will be impaired. To avoid problems, ensure another global catalog server is available or designate a new one.
- Don’t accidentally remove the last global catalog server from a site. If you remove the last global catalog server from a site, computers in the site will query a global catalog server in another site when searching for resources in other domains in the forest, and a domain controller responding to a user’s logon or authentication request will need to obtain the required information from a global catalog server in another site. To avoid problems, ensure another global catalog server is available, designate a new one, or verify the affected site is connected to other sites with fast, reliable links.
- Determine whether a domain controller is acting as a global catalog server by typing the following at a command prompt: `dsquery server -domain DomainName | dsget server -isgc -dnsname` where `DomainName` is the name of the domain you want to examine. The resulting output lists all global catalog servers in the domain.

Bridgehead server

- Don’t accidentally remove the last preferred bridgehead server from a site. If you remove the last preferred bridgehead server, intersite replication will stop until you change the preferred bridgehead server configuration options.
You can avoid problems by (1) removing the preferred bridgehead server designation prior to demoting the domain controller and thereby allowing Active Directory to select the bridgehead servers to use, or (2) ensuring one or more additional preferred bridgehead servers are available.

- Determine whether a domain controller is acting as a bridgehead server by typing the following at a command prompt: `repadmin /bridgeheads site:SiteName` where SiteName is the name of the site, such as repadmin /bridgeheads site:Seattle-First-Site. The resulting output is a list of bridgehead servers in the specified site. If you omit the site:SiteName value, the details for the current site are returned.

**Operations master**

- Don’t accidentally demote a domain controller holding a forestwide or domainwide operations master role. If you remove an operations master without first transferring the role, Active Directory will try to transfer the role as part of the demotion process, and the domain controller that ends up holding the role may not be the one you would have selected.
- Determine whether a domain controller is acting as an operations master by typing the following at a command prompt: `netdom query fsmo`. The resulting output lists the forestwide and domainwide operations master role holders.

Before you remove the last domain controller in a domain, you should examine domain accounts and look for encrypted files and folders. Because the deleted domain will no longer exist, its accounts and cryptographic keys will no longer be applicable, and this results in the deletion of all domain accounts and all certificates and cryptographic keys. You must decrypt any encrypted data on the server, including data stored using the Encrypting File System (EFS), before removing the last domain controller, or the data will be permanently inaccessible.

You can check for encrypted files and folders by using the EFSInfo utility. At a command prompt, enter `efsinfo /s:DriveDesignator /i | find “: Encrypted”` where DriveDesignator is the drive designator of the volume to search, such as C:.

The credentials you need to demote a domain controller depend on the domain controller’s functions and roles. Keep the following in mind:

- To remove the last domain controller from a domain tree or child domain, you must use an account that is a member of the Enterprise Admins group or be able to provide credentials for an enterprise administrator account.
- To remove the last domain controller in a forest, you must log on to the domain as Administrator or use an account that is a member of the Domain Admins group.
- To remove other domain controllers, you must use an account that is a member of either the Enterprise Admins or Domain Admins group.
Removing Additional Domain Controllers

You can remove an additional domain controller from a domain by completing the following steps:

1. Start the Active Directory Domain Services Installation Wizard by clicking Start, typing `dcpromo` in the Search box, and pressing Enter.

2. When the wizard starts, it will confirm that the computer is a domain controller. You should see a message stating the server is already a domain controller and that by continuing you will remove Active Directory, as shown in Figure 3-7. Click Next.

   ![Figure 3-7](image)
   
   **Figure 3-7** Initiate Active Directory removal.

3. If the domain controller is a global catalog server, a message appears to warn you about ensuring other global catalog servers are available, as shown in Figure 3-8. Before you click OK to continue, you should ensure one or more global catalog servers are available, as discussed previously.

   ![Figure 3-8](image)
   
   **Figure 3-8** Ensure that you don’t accidentally remove the last global catalog server.
4. On the Delete The Domain page, click Next without making a selection. If the domain controller is the last in the domain, you’ll see a warning like the one shown in Figure 3-9. In this case, I recommend clicking No and then clicking Cancel, which will exit the wizard and allow you to perform any necessary preparatory tasks if you do indeed want to remove the last domain controller. When you are ready to proceed, you should perform the tasks discussed in “Removing the Last Domain Controller,” later in this chapter.

![Active Directory Domain Services Installation Wizard]

FIGURE 3-9 Ensure that you don’t accidentally remove the last domain controller.

5. If the domain controller is the last DNS server for one or more Active Directory–integrated zones, a message appears to warn you that you may be unable to resolve DNS names in the applicable zones. Before continuing by clicking OK, you should ensure that you establish another DNS server for these zones.

6. If the domain controller has application directory partitions, the next page you will see is the Application Directory Partitions page, shown in Figure 3-10. You will need to do the following:
   a. If you want to retain any application directory partitions that are stored on the domain controller, you will need to use the application that created the partition to extract and save the partition data as appropriate. If the application does not provide such a tool, you can let the Active Directory Domain Services Installation Wizard remove the related directory partitions. When you are ready to continue with Active Directory removal, you can click Refresh to update the list and see any changes.
   b. Click Next. Confirm that you want to delete all application directory partitions on the domain controller by selecting the related option and then clicking Next. Keep in mind that deleting the last replica of an application partition will delete all data associated with that partition.

7. The wizard checks DNS to see if any active delegations for the server need to be removed. If the Remove DNS Delegation page is displayed, as shown in Figure 3-11, verify that the Delete The DNS Delegations Pointing To This Server check box is selected. Then click Next. If you don’t remove the delegations at this time, you’ll need to manually remove them later using the DNS console.
FIGURE 3-10 Ensure that you don’t accidentally remove the last replica of application partitions.

FIGURE 3-11 Verify that you want to remove DNS delegations.
8. If you are removing DNS delegations, the Active Directory Domain Services Installation Wizard then examines the DNS configuration, checking your credentials and attempting to contact a DNS server in the domain. If you need additional credentials to remove DNS delegations, the Windows Security dialog box is displayed. Enter administrative credentials for the server that hosts the DNS zone in which the domain controller is registered and then click OK.

9. On the Administrator Password page, you are prompted to type and confirm the password for the local Administrator account on the server. You need to enter a password for the local Administrator account because domain controllers don’t have local accounts but member or stand-alone servers do, so the local Administrator account will be re-created as part of the Active Directory removal process. Click Next.

10. On the Summary page, review your selections. Optionally, click Export Settings to save these settings to an answer file that you can use to perform unattended demotion of other domain controllers. When you click Next again, the wizard uses the options you’ve selected to demote the domain controller. This process can take several minutes.

**NOTE** If there are updates to other domains in the forest that have not been replicated, the domain controller replicates these updates, and then the wizard begins the demotion process. If the domain controller is also a DNS server, the DNS data in the ForestDnsZones and DomainDnsZones partitions is removed. If the domain controller is the last DNS server in the domain, this results in the last replica of the DNS information being removed from the domain. All associated DNS records are lost and may need to be re-created.

11. On the Completing The Active Directory Domain Services Installation Wizard page, click Finish. You can either select the Reboot On Completion check box to have the server restart automatically, or you can restart the server to complete the Active Directory removal when you are prompted to do so.

When removing an additional domain controller from a domain, the Active Directory Domain Services Installation Wizard does the following:

- Removes Active Directory and all related services from the server and makes it a member server in the domain
- Changes the computer account type and moves the computer account from the Domain Controllers container in Active Directory to the Computers container
- Transfers any operations master roles from the server to another domain controller in the domain
- Updates DNS to remove the domain controller SRV records
- Creates a local Security Accounts Manager (SAM) account database and a local Administrator account
**REAL WORLD** When you remove a domain controller, the related server object is removed from the domain directory partition automatically. However, the server object representing the retired domain controller in the configuration directory partition can have child objects and is therefore not removed automatically. For more information on these objects, refer to “Confirming Removal of Deleted Server Objects,” later in this chapter.

Removing the Last Domain Controller

You can remove the last domain controller in a domain or forest by completing the following steps:

1. Start the Active Directory Domain Services Installation Wizard by clicking Start, typing `dcpromo` in the Search box, and pressing Enter.

2. When the wizard starts, click Next. If the domain controller is a global catalog server, a message appears to warn you about ensuring other global catalog servers are available. Click OK to continue.

3. On the Delete The Domain page, select Delete The Domain Because This Server Is The Last Domain Controller In The Domain check box, as shown in Figure 3-12. Click Next to continue. After you remove the last domain controller in a domain or forest, you can no longer access any directory data, Active Directory accounts, or encrypted data.

![Active Directory Domain Services Installation Wizard](image)

*FIGURE 3-12* Verify that you want to delete the domain or forest.
4. The rest of the installation proceeds as previously discussed. Continue with steps 6 through 11 of the previous section, “Removing Additional Domain Controllers.” Note the following:

- If you are removing the last domain controller from a domain, the wizard verifies that there are no child domains of the current domain before performing the removal operation. If child domains are found, removal of Active Directory fails, with an error telling you that you cannot remove Active Directory.
- When the domain being removed is a child domain, the wizard notifies a domain controller in the parent domain that the child domain is being removed. For a parent domain in its own tree, a domain controller in the forest root domain is notified. Either way, the domain object is tombstoned, and this change is then replicated to other domain controllers. The domain object and any related trust objects are also removed from the forest.
- As part of removing Active Directory from the last domain controller in a domain, all domain accounts, all certificates, and all cryptographic keys are removed from the server. The wizard creates a local SAM account database and a local Administrator account. It then changes the computer account type to a stand-alone server and puts the server in a new workgroup.

Removing Domain Controllers Using Answer Files or the Command Line

On a Full Server or Core Server installation of Windows Server 2008, you can remove domain controllers using an unattended removal or the command line. You must be logged on as the Domain Admins group in the domain.

With the unattended removal method, you must first prepare an answer file that contains the desired removal values. You can create an answer file for removing a domain controller by completing the following steps:

1. Open Notepad or any other text editor.
2. On the first line, type `[DCINSTALL]`, and then press Enter.
3. Type the following entries, one entry on each line.

```
UserName=AdminAccountInDomainOfDC
UserDomain=DomainOfAdminAccount
Password="PasswordOfAdminAccount"
AdministratorPassword=NewLocalAdminPassword
RemoveApplicationPartitions=yes
RetainDCMetadata=No
RemoveDNSDelegation=yes
RebootOnCompletion=yes
```
4. If the account that is being used to remove AD DS is different from the account in the parent domain that has the privileges that are required to remove a DNS delegation, you must specify the account that can remove the DNS delegation by entering the following additional parameters.

   DNSDelegationUserName=DelegationAdminAccount
   DNSDelegationPassword="Password"

5. If the domain controller is the last DNS server for one or more Active Directory–integrated DNS zones that it hosts, Dcpromo will exit with an error. You can force Dcpromo to proceed by entering the following additional parameter.

   IgnoreIsLastDNSServerForZone=yes

6. If the domain controller is the last in the domain or forest, Dcpromo will exit with an error. You can force Dcpromo to proceed by entering the following additional parameter.

   IsLastDCInDomain=yes

   **NOTE** If there is actually another domain controller in the domain, Dcpromo will exit with a mismatch error. Typically, this is what you’d want to happen. However, you can force Dcpromo to continue with the removal as if this were the last domain controller by using IgnoreIsLastDCInDomainMismatch=Yes.

7. Save the answer file as a .txt file and then copy the file to a location accessible from the server you want to promote.

8. After you create the answer file, you can start the unattended removal by entering the following at a command prompt:

   dcpromo /unattend:"PathToAnswerFile"

   where PathToAnswerFile is the full file path to the answer file, such as C:\data\removedc.txt.

   At the command line, you can remove a domain controller from a domain using the following command.

   dcpromo /unattend
   /UserName:AdminAccountInDomainOfDC
   /UserDomain:DomainOfAdminAccount
   /Password:"PasswordOfAdminAccount"
   /AdministratorPassword:NewLocalAdminPassword
   /RemoveApplicationPartitions:yes
   /RetainDCMetadata:No
   /RemoveDNSDelegation:yes
   /RebootOnCompletion:yes

96  CHAPTER 3  Deploying Writable Domain Controllers
If the domain controller is the last DNS server for one or more Active Directory–
integrated DNS zones that it hosts, Dcpromo will exit with an error. You can force
Dcpromo to proceed using the following additional parameter.

/IgnoreIsLastDNSServerForZone:yes

If the domain controller is the last in the domain or forest, Dcpromo will exit
with an error. You can force Dcpromo to proceed using the following additional
parameter.

/IsLastDCInDomain:yes

When the unattended removal or command-line execution completes, Dcpromo
exits with a return code. A return code of 1 to 10 indicates success. A return code of
11 to 100 indicates failure. Note any related error text and take appropriate correct-
tive action as necessary.

Forcing the Removal of Domain Controllers

A domain controller must have connectivity to other domain controllers in the
domain in order to demote the domain controller and successfully remove Ac-
tive Directory Domain Services. If a domain controller has no connectivity to other
domain controllers, the standard removal process will fail, and you will need to con-
nect the domain controller to the domain and then restart the removal process. In
a limited number of situations, however, you might not want or be able to connect
the domain controller to the domain and instead might want to force the removal
of the domain controller.

Forcing the removal of a domain controller is a three-part process. You must:

1. Restart the domain controller in Directory Services Restore Mode.
2. Perform the forced removal of the domain controller.
3. Clean up the Active Directory forest metadata.

These tasks are discussed in the sections that follow.

Restarting a Domain Controller in Directory Services Restore
Mode

Before you can forcibly remove Active Directory Domain Services, you must restart
the domain controller in Directory Services Restore Mode. Restarting in this mode
takes the domain controller offline, meaning it functions as a member server, not
as a domain controller. During installation of Active Directory Domain Services, you
set the Administrator password for logging on to the server in Directory Services
Restore Mode.
You can restart a domain controller in Directory Services Restore Mode manually by pressing the F8 key during domain controller startup. You must then log on by using the Directory Services Restore Mode password for the local Administrator account. A disadvantage of this technique is that if you accidentally restart the domain controller, you might forget to put it back into Directory Services Restore Mode.

To ensure the domain controller is in Directory Services Restore Mode until you specify otherwise, you can use the System Configuration utility or the Boot Configuration Data (BCD) editor to set a Directory Repair flag. Once this flag is set, the domain controller will always start in Directory Services Restore Mode, and you can be sure that you won’t accidentally restart the domain controller in another mode.

To restart a domain controller in Directory Services Restore Mode using the System Configuration utility, complete the following steps:

1. On the Start menu, point to Administrative Tools, and then click System Configuration.
2. On the Boot tab, in Boot Options, select Safe Boot, and then click Active Directory Repair, as shown in Figure 3-13.
3. Click OK to exit the System Configuration utility and save your settings.
4. Restart the domain controller. The domain controller restarts in Directory Services Restore Mode.

When you have finished performing procedures in Directory Services Restore Mode, restart the domain controller in normal mode by completing the following steps:

1. On the Start menu, point to Administrative Tools, and then click System Configuration.
2. On the General tab, in Startup Selection, click Normal Startup, and then click OK.

3. The domain controller restarts in normal mode.

To restart a domain controller in Directory Services Restore Mode using the BCD editor, complete the following steps:

1. Click Start, right-click Command Prompt, and then click Run As Administrator to open an elevated command prompt.

2. At the command prompt, enter the following command: `bcdedit /set safeboot disrepair`. This configures the boot process to start in Directory Services Restore Mode.

3. At the command prompt, enter the following command: `shutdown -t 0 -r`. This shuts down the server and restarts it without delay.

When you have finished performing procedures in Directory Services Restore Mode, restart the domain controller in normal mode by completing the following steps:

1. Click Start, right-click Command Prompt, and then click Run As Administrator to open an elevated command prompt.

2. At the command prompt, you need to enter the following command: `bcdedit /deletevalue safeboot`. This deletes the safeboot value and returns the boot process to the previous setting.

3. At the command prompt, enter the following command: `shutdown -t 0 -r`. This shuts down the server and restarts it without delay.

Performing Forced Removal of Domain Controllers

You can force the removal of a domain controller by completing the following steps:

1. Click Start, right-click Command Prompt, and then click Run As Administrator to open an elevated command prompt.

2. At the command prompt, enter the following command: `dcpromo /forceremoval`. This starts the Active Directory Domain Services Installation Wizard in Force Removal mode.

3. If the domain controller hosts any operations master roles, is a DNS server, or is a global catalog server, warnings similar to the one shown in Figure 3-14 are displayed to explain how the forced removal of the related function will affect the rest of the environment. After you review the recommendations and take appropriate actions (if possible), click Yes to continue.
FIGURE 3-14 Review each removal warning in turn.


5. On the Force The Removal Of Active Directory Domain Services page, shown in Figure 3-15, review the information about forcing the removal of Active Directory Domain Services and the required metadata cleanup operations, and then click Next.

FIGURE 3-15 Review the forced removal warning.
6. If the domain controller is a DNS server with zones integrated with Active Directory, you’ll see a warning stating one or more Active Directory–integrated zones will be deleted. Before continuing by clicking OK, you should ensure that there is another DNS server for these zones. Also note that you’ll need to manually remove DNS delegations pointing to this server.

7. On the Administrator Password page, you are prompted to type and confirm the password for the local Administrator account on the server. You need to enter a password for the local Administrator account because domain controllers don’t have local accounts, but member or stand-alone servers do, so the local Administrator account will be re-created as part of the Active Directory removal process. Click Next.

8. On the Summary page, review your selections. Optionally, click Export Settings to save these settings to an answer file that you can use to perform unattended forced removal of other domain controllers. When you click Next again, the wizard uses the options you’ve selected to forcibly remove Active Directory Domain Services. This process can take several minutes.

9. On the Completing The Active Directory Domain Services Installation Wizard page, click Finish. Do not select the Reboot On Completion check box. When you are prompted to restart the server, do not do so. Instead, you’ll want to examine the server and perform any necessary additional tasks. Then when you are finished, restart the server in normal mode using the appropriate technique discussed previously.

When forcibly removing a domain controller from a domain, the Active Directory Domain Services Installation Wizard does the following:

- Removes Active Directory and all related services from the server
- Changes the computer account type
- Creates a local Security Accounts Manager (SAM) account database and a local Administrator account

At the command line, you can force the removal of a domain controller from a domain using the following command.

```
dcpromo /unattend /forceremoval
/AdministratorPassword:NewLocalAdminPassword
/RemoveApplicationPartitions:yes
/RemoveDNSDelegation:yes
/RebootOnCompletion:yes
```

If the domain controller is an operations master, Dcpromo will exit with an error. You can force Dcpromo to proceed using the following additional parameter.

```
/DemoteFSMO:yes
```
This option should also suppress errors related to the domain controller being a global catalog server, a DNS server, or both.

When the command-line execution completes, Dcpromo exits with a return code. A return code of 1 to 10 indicates success. A return code of 11 to 100 indicates failure. Note the related error text and take appropriate corrective action as necessary.

Cleaning Up Metadata in the Active Directory Forest

When you force the removal of a disconnected domain controller, the Active Directory forest metadata is not updated automatically as it is when a domain controller is removed normally. Because of this, you must manually update the forest metadata after you remove the domain controller.

You perform metadata cleanup on a domain controller in the domain of the domain controller that you forcibly removed. During metadata cleanup, Active Directory automatically performs the following tasks:

- Removes data from the directory that identifies the retired domain controller to the replication system
- Removes any related File Replication Service (FRS) and Distributed File System (DFS) Replication connections
- Attempts to transfer or seize any operations master roles that the retired domain controller holds

Cleaning Up Server Metadata

On domain controllers that are running Windows Server 2008, you can use Active Directory Users and Computers to clean up server metadata. Deleting the computer object in the Domain Controllers organizational unit (OU) initiates the cleanup process, and all related tasks are performed automatically. Using Active Directory Users and Computers, you can clean up metadata by completing the following steps:

1. Open Active Directory Users and Computers by clicking Start, clicking Administrative Tools, and then clicking Active Directory Users And Computers.
2. You must be connected to a domain controller in the domain of the domain controller that you forcibly removed. If you aren’t or are unsure, right-click the Active Directory Users And Computers node and then click Change Domain Controller. Click the name of a domain controller in the appropriate domain, and then click OK.
3. Expand the domain of the domain controller that you forcibly removed, and then click Domain Controllers.
4. In the details pane, right-click the computer object of the retired domain controller, and then click Delete.
5. In the Active Directory Domain Services dialog box, click Yes to confirm that you want to delete the computer object.
6. In the Deleting Domain Controller dialog box, select This Domain Controller Is Permanently Offline And Can No Longer Be Demoted, and then click Delete.

7. If the domain controller was a global catalog server, in the Delete Domain Controller dialog box, click Yes to continue with the deletion.

8. If the domain controller currently holds one or more operations master roles, click OK to move the role or roles to the domain controller that is shown. Although you cannot change this domain controller at the present time, you can move the role once the metadata cleanup procedure is completed.

On domain controllers that are running Windows Server 2003 with Service Pack 1 (SP1), Windows Server 2003 with Service Pack 2 (SP2), Windows Server 2003 R2, or Windows Server 2008, you also can perform metadata cleanup by using the Ntdsutil command-line tool. Using Ntdsutil, you can clean up server metadata by completing the following steps:

1. Click Start, right-click Command Prompt, and then click Run As Administrator to open an elevated command prompt.

2. At the command prompt, enter the following command: `ntdsutil`.

3. At the ntdsutil prompt, enter the following command: `metadata cleanup`.

4. At the metadata cleanup prompt, enter the following command if you are logged on to the domain of the domain controller that you forcibly removed: `remove selected server RetiredServer` where `RetiredServer` is the distinguished name of the retired domain controller. Otherwise, enter the following command: `remove selected server RetiredServer on Target-Server` where `RetiredServer` is the distinguished name of the retired domain controller and where `TargetServer` is the DNS name of a domain controller in the domain of the domain controller that you forcibly removed.

   **REAL WORLD** This process initiates removal of objects that refer to the retired domain controller and then removes those objects from a specified server. Once the changes are replicated, the related objects will be removed throughout the Active Directory forest. You must identify the retired server by its distinguished name, such as “CN=CorpServer27,OU=Domain Controllers,DC=cpandl,DC=com”. If you specify a target server, you must use the DNS name of the domain controller to which you want to connect, such as “CorpServer27.Cpandl.com”. If you do not specify a target server, the objects are removed from the domain controller to which you are currently connected.

5. When prompted with the Server Remove Configuration dialog box, read the details provided. Click Yes to remove the server object and related metadata. Ntdsutil will then confirm that the server object and related metadata was removed successfully. If you receive an error message that indicates that the object cannot be found, the server object and related metadata might have been removed previously.
6. At the metadata cleanup prompt, enter the following command: quit.
7. At the ntdsutil prompt, enter the following command: quit.

Confirming Removal of Deleted Server Objects

When you remove a domain controller, the related server object is removed from the domain directory partition automatically. You can confirm this using Active Directory Users and Computers. However, the server object representing the retired domain controller in the configuration directory partition can have child objects and is therefore not removed automatically. You can confirm the status of the server object in the configuration directory partition by using Active Directory Sites And Services.

You can confirm removal of server objects for a retired domain controller by completing the following steps:

1. Open Active Directory Users and Computers by clicking Start, clicking Administrative Tools, and then clicking Active Directory Users And Computers.
2. Expand the domain of the domain controller that you forcibly removed, and then click Domain Controllers.
3. In the details pane, the computer object of the retired domain controller should not appear. If it does, follow the steps in “Cleaning Up Server Metadata,” earlier in this chapter, to remove the object using Active Directory Users and Computers.
4. Open Active Directory Sites and Services by clicking Start, clicking Administrative Tools, and then clicking Active Directory Sites And Services.
5. Any domain controllers associated with a site are listed in the site’s Servers node. Select the site that the retired domain controller was previously associated with and then expand the related Servers node.
6. Confirm that the server object for the retired domain controller does not contain an NTDS Settings object. If no child objects appear below the server object, you can delete the server object. Right-click the server object and then click Delete. When prompted to confirm, click Yes.

**REAL WORLD** Do not delete the server object if it has a child object. If an NTDS Settings object appears below the server object, either replication on the domain controller on which you are viewing the configuration container has not occurred or the domain controller was not properly decommissioned. If a child object other than NTDS Settings is listed, another application has published the object. You must contact the appropriate application administrator and determine the required actions to remove the child object.
A resource records, 34, 204
AAAA resource records, 204
AB performance counters, 218
access control
adding domain local groups, 153
adding global groups, 153
functionality, 5
accounts. See specific user accounts
Active Directory, 3, 5, 22–27
Active Directory Administrative Center, 26
Active Directory Domain Services. See AD DS
Active Directory Domain Services Installation Wizard. See Dcpromo.exe
Active Directory Domains And Trusts tool
configuring name suffix routing, 165–166
configuring UPN name suffixes, 164
examining trusts, 234–235
functionality, 24
locating domain naming masters, 172
New Trust Wizard, 236–239
one-way incoming external trusts, 241
one-way incoming forest trusts, 248
one-way incoming realm trusts, 251
one-way incoming shortcut trusts, 244–245
one-way outgoing external trusts, 242
one-way outgoing forest trusts, 249
one-way outgoing realm trusts, 252
one-way outgoing shortcut trusts, 245–246
Protect Object From Accidental Deletion option, 259
removing manually created trusts, 253
resetting trusts, 254–255
selective authentication for external trusts, 256
selective authentication for forest trusts, 256–257
setting functional levels, 261–262
transferring domain naming masters, 172–173
two-way external trusts, 243–244
two-way forest trusts, 250–251
two-way realm trusts, 252–253
two-way shortcut trusts, 246–247
Active Directory Installation Wizard, 7–8
Active Directory Schema tool
changing schemas, 180–181
functionality, 25, 159–162
Active Directory Sites And Services tool
adding domain controllers to sites, 203
adding global catalog servers, 142–143
configuring bridgehead servers, 215
configuring link replication schedules, 210–212
creating site links, 208–209
creating sites, 200–201
creating subnets, 200, 202
enabling universal group membership caching, 153–155
functionality, 24
generating replication topology, 222
identifying global catalog servers, 149
identifying standby operations master, 182
locating ISTGs, 216
managing site links, 206
moving domain controllers, 205
optimizing site link configurations, 217–218
Protect Object From Accidental Deletion option, 259
removing global catalog servers, 151
site link bridging, 212–213
verifying and forcing replication, 222–223
Active Directory Users And Computers tool
Advanced mode, 128–129
checking for updates, 49, 115
cleaning up server metadata, 102–104
creating RODC account, 120–121
drafting Password Replication Policy, 130–132
functionality, 24
granting Allowed To Authenticate permission, 257
identifying allowed/denied accounts, 133
locating infrastructure masters, 174
locating POC emulators, 176
locating RID masters, 178
managing credentials on RODCs, 132–133
Protect Object From Accidental Deletion option, 259
resetting computer account passwords, 282
resetting credentials, 134
transferring infrastructure masters, 174–175
transferring POC emulators, 176–177
transferring RID masters, 179
Active Directory-integrated DSN zone, 108, 281
AD DS (Active Directory Domain Services)
adding roles, 8
authoritative restores, 278–279, 282–285
backup up/restoring system state, 280–281
backups supported, 278
decommissioning domain controllers, 73
Deleted Item Retention lifetime, 262
installing binaries, 41, 74, 76
maintaining directory database, 286–291
moving directory database, 290–293
nonauthoritative restores, 278, 281–282
offline defragmentation, 288–290
restartable feature, 260
restoring SYSVOL data, 285–286
starting/stopping, 260–261
triggering cache refresh, 156
Add Feature Wizard, 24, 277
Add Role Wizard, 8
Address Book, 218
Administrator account
Administrators group, 23
creating domain controllers, 41
functionality, 23
removing additional domain controllers, 89
Administrators group
Administrator account, 23
Enterprise Admins group, 23
functionality, 23
viewing schema, 159
ADPREP command, 40
ADPREP DOMAINPREP command, 27, 41
ADPREP FORESTPREP command, 27, 40
ADPREP GPPREP command, 27, 108
ADPREP RODCPREP command, 40, 108
ADSI Edit tool, 25, 262
Advanced Encryption Standard (AES), 38
AES (Advanced Encryption Standard), 38
Allowed Accounts list, 128
Allowed RODC Password Replication Group, 129–130
Allowed To Authenticate permission

Allowed To Authenticate permission, 256–257
answer files
adding RODCs using, 115–119
adding writable domain controllers using, 85–87
removing domain controllers using, 95–97
staged installations using, 123–126
AsyncThreadQueue, 218
ATQ performance counters, 218
attributes. See also specific attributes
activating, 39
for objects, 11
indexing, 162
Password Replication Policy, 128
redefining, 39
replication, 158–163
RODC support, 106
Authenticated To list, 128
Authenticated Users group, 228
authentication. See also Kerberos authentication; selective authentication
across domain boundaries, 232
across forest boundaries, 232–233
cross-forest, 37
domainwide, 238, 255
foretwide, 239, 255
global catalog servers, 74, 141
logon process and, 192, 230
name suffix routing, 163, 165
overview, 229–231
PDC emulators, 175
replication model, 192
SID support, 140, 152–153
site considerations, 16, 190
time synchronization and, 263
trust paths, 228
authoritative restores
functionality, 278–279, 282–285
SYSVOL data, 285
authorization
Kerberos support, 5
role-based, 39
stored policies, 37
backup and restore procedures
AD DS support, 278–279
authoritative restores, 278–279, 282–285
critical-volume backups, 278, 282
full server backups, 208, 278, 281
global catalog servers, 150
nonauthoritative restores, 278, 281–282
standby operations masters, 168
system state backups, 278, 280–281
bandwidth
intersite replication, 194, 198–199
intrasite replication, 194
multiple site replication, 192
setting link costs, 208
site boundary considerations, 191
site design considerations, 197
time synchronization, 264
BCD editor, 98–99
BitLocker Drive Encryption, 162
branch offices, 109, 119
bridgehead servers changing, 214
configuring, 214–215
decommissioning domain controllers, 88–89
designating, 214–215
functionality, 190
intersite replication, 192, 195–196, 207
ISTG support, 196
locating, 213–214, 221
moving domain controllers, 204–205
replication interval, 208
RODC considerations, 106
bridging site links, 197, 212–213
BuiltIn container, 49
C

caching credentials, 141
universal group memberships,
141–142, 152–157, 229
Cert Publishers group, 130
certificate authorities
site considerations, 35, 190
SMTP support, 207
child domains
adding to forests, 33
creating, 66–71
name suffix routing, 165
removing additional domain controllers, 89
trust considerations, 232
classes, 12, 39
command-line tools. See also specific commands/tools
adding RODCs using, 115–119
adding writable domain controllers using, 85–87
functionality, 27
removing domain controllers using, 95–97
staged installations using, 123–126
common name (CN), 30
calendar accounts, 278, 282
Computer object class, 12–13
computer objects, 11
Computers container, 37–38, 49
Computers object, 11
Configuration container, 30
classification partitions, 31, 34
configuring
bridgehead servers, 214–215
deleted item retention, 262–263
DNS, 7–8
DNS servers, 7
domain controllers, 9, 41
intersite replication, 206–218
name suffix routing, 165–166
Password Replication Policy, 127, 129
replication schedules, 210–212
selective authentication, 255–257
site links, 35, 206–218
sites, 200–206
subnets, 200–206
UPN name suffixes, 164–165
Windows Time service, 265–266, 269–277
conflict resolution, 10
certificates
connection objects, 221
constrained delegation, 37–38
container objects, 11
credentials
adding RODCs using, 115–119
caching, 141
resetting, 134
RODC considerations, 106
site links, 183–188
critical-volume backups, 278, 282
cross-forest authentication, 37
cross-forest trusts. See forest trusts
D

database management
checking for free disk space, 287–288
DSRM support, 260
moving directory database, 290–293
offline defragmentation, 288–290
operations overview, 287
DC Locator process, 205–206
DCDIAG command
functionality, 295
monitoring replication process, 144
troubleshooting operations masters, 187–188
DCGPOFix command, 295
DCLList, 220
Dcpromo.exe tool
adding RODCs using replication, 109–115
adding writable domain controllers, 76–83
AllowDomainControllerReinstall parameter, 52
AllowDomainReinstall parameter, 52
ApplicationPartitionsToReplicate parameter, 52
ChildName parameter, 52
calendar accounts, 278, 282
 configuring services, 74
ConfirmGc parameter, 53
CreateDNSDelegation parameter, 53
creating child domains, 66–71
creating domain trees, 59–66
creating forests, 42–59
CriticalReplicationOnly parameter, 53
DatabasePath parameter, 53
DCAccountName parameter, 53
decommissioning operations masters, 183
DelegatedAdmin parameter, 53
DNSDelegationPassword parameter, 54
Deleted Object Recovery, 39
deletion
AD DS objects, 287
global catalogs, 287
objects marked for, 280
protecting from accidental, 259–260
Denied Accounts list, 128
Denied RODC Password Replication Group, 129–130
Deny Delete Subtree permission, 259
Description attribute, 13
DFS (Distributed File System)
cleaning up metadata in forests, 102
domain controller support, 21, 37
domain functional levels, 37–38
replication support, 193
service dependencies, 219
site considerations, 35, 190
stopping AD DS, 261
SYSVOL replication, 219
DFS Replication log, 219
DFS (DFS Service), 219
DHCP (Dynamic Host Configuration Protocol)
dynamic IP addresses, 200
site considerations, 35, 190
Direction Replication Agent, 219
directory defined, 3
distinguished names, 30
domain controllers, 8
domain support, 17
object class support, 12
directory partitions
bridgehead servers, 214
defined, 30
domain controllers and, 31
domains and, 30
Event ID 1704, 163
functionality, 30–31
lists replication partners, 221
RODC considerations, 106–107
synchronizing, 163
Directory Service log
Event ID 1046, 290
Event ID 116, 290
Event ID 1268, 151
Event ID 1646, 287
Event ID 16645, 177
Event ID 16651, 177–178
Event ID 1668, 155
Event ID 1702, 163
Event ID 1703, 163
Event ID 1704, 163
functionality, 151
monitoring replication, 219
directory services functionality, 3–4, 139
performance counters, 219
Directory Services Restore Mode.
See DSRM (Directory Services Restore Mode)
directory trees, 30
DirectoryServices performance object, 218–219
disaster recovery
AD DS considerations, 278–279
domain controller considerations, 33, 278–279
DISKPART command, 296
distinguished name (DN), 30, 173
Distributed File System. See DFS (Distributed File System)
DN (distinguished name), 30, 173
DNS (Domain Name System). See also SRV resource records
cleaning up old references, 286
directory partitions, 31
external trusts, 240
functionality, 6–8
handling updates, 7, 83
installing and configuring, 7–8
name suffix routing, 165
replication support, 193
service dependencies, 219
site considerations, 35, 198
UPN considerations, 141
verifying global catalog servers, 147
DNS servers configuring, 7
determining placement, 34
dynamic IP addresses, 41
external trusts, 240
functionality, 7–8
moving domain controllers, 204
operations masters, 183
RODC considerations, 106, 108
site considerations, 190
static IP addresses, 34
Domain Admins group
adding global catalog servers, 142
adding writable domain controllers, 85
Administrator account, 23
Administrators group, 23
establishing domain trusts, 236
functionality, 23
identifying standby operations master, 182
managing Password Replication Policy, 130
removing additional domain controllers, 89
removing domain controllers, 95
RODC considerations, 130
staged installations, 119
viewing schema, 159
domain controllers. See also
RODCs (read-only domain controllers); writable domain controllers
adding to default sites, 200
adding to sites, 203–205
authentication process, 231
bridgehead servers, 88–89
cache support, 229
cleaning up metadata in forests, 97, 102–104
configuration partitions, 31, 34
configuring, 9, 41
configuring as time source, 268
conflict resolution, 10
creating, 41
DC Locator process, 205–206
decommissioning, 73, 88–97
dedicated, 279
defined, 8
demoting, 89
Domain Controllers group

directory partitions, 31

disaster recovery considerations, 33, 278–279
displaying connection objects, 221
domain naming master, 168
dynamic IP addresses, 41
easy renaming, 37–38
encrypted data considerations, 42, 76
forcing removal, 97–104
functionality, 10
global catalog servers, 74, 88, 139
identifying as standby operations master, 181
installing, 42–59, 168, 286
listing computers with opened sessions, 221
listing server certificates, 221
logically apportioning data, 31
multimaster replication, 9
nondedicated, 279
operations masters, 74, 89, 168–169, 174
preparing for decommissioning, 73–74, 88–89
preparing for deployment, 73–74
removing additional, 90–93
removing last, 94–95
removing using answer files/commands line, 95–97
replicating changes, 8, 10, 21, 31, 191
replicating SYSENV, 193
restarting in DSRM, 97–99, 260, 288–291–292
restoring AD DS, 278–279, 281–282
RID masters, 177
rootDSE, 30
schema considerations, 34
schema masters, 168
schema partitions, 31
site support, 16, 35, 74, 190
time synchronization, 264
tracking USNs, 220
trust paths, 228
updating membership cache, 156
verifying trusts, 254
Domain Controllers group, 130
domain forests. See forests
domain functional levels defined, 36
features available, 36–37
level support, 18, 36
RODC considerations, 107
setting, 18, 261–262
domain local groups, 153, 229
Domain Name System. See DNS
(Domain Name System)
domain names, 17, 148
domain naming masters
domain controllers, 168
functionality, 168
in forests, 168
locating, 172
managing, 172–173
placement considerations, 170
transferring roles, 172–173
domain partitions
bridgehead servers, 214
replicating changes, 191
SMTP limitations, 207
Domain Rename tool (Rendom. exe), 33
domain schemas, 40
domain trees
adding to forests, 33
as logical components, 16, 18
creating, 59–66
domain forests support, 20
removing additional domain controllers, 89
trust considerations, 228–229
domain trusts, 236
Domain Users group, 23
DomainControllers container, 49
DomainDNSZones, 106
domainDNS object class, 30
domains
Active Directory, 5
adding RODCs, 108–119
as logical components, 16–18
authentication across boundaries, 232
child, 33, 66–71, 89, 165, 232
configuring domain controllers, 9
creating hierarchies, 21, 33
defined, 5, 16
directory partitions, 30
DNS, 6–8
establishing infrastructure, 32–34
functionality, 5
global catalog servers, 35
infrastructure master, 168
listing trusted, 221
operations masters, 168
organizational, 6
parent, 7, 232
PDC emulator, 168
preparing, 40–41
RID master, 168
root, 6, 18, 20
time synchronization, 264
top-level, 6–7
trusted, 20, 228–229
DSRM command, 27, 301
DSQUERY COMPUTER command, 301
DSQUERY CONTACT command, 301
DSQUERY GROUP command, 302
DSQUERY PARTITION command, 302
DSQUERY QUOTA command, 302
DSQUERY SERVER command
decommissioning domain controllers, 88
determining servers associated with sites, 203
functionality, 302
listing domain controllers, 204
DSQUERY SITE command, 303
DSQUERY USER command, 303
DSRM (Directory Services Restore Mode)
authoritative restore, 279, 284
backing up/restoring system state, 280
nonauthoritative restores, 281
restoring domain controllers, 97–99, 260, 288–291–292
setting password, 116
stopping AD DS, 260
DSRM command, 27, 304
Dynamic Host Configuration Protocol (DHCP)
dynamic IP addresses, 200
site considerations, 35, 190
dynamic IP addresses, 41, 200
E

easy DC renaming, 37
EFS (Encrypting File System)
domain controller considerations, 42, 76
RODC considerations, 107
EFSInfo tool
adding writable domain controllers, 76
checking for encrypted files, 42
decommissioning domain controllers, 89
RODC deployment, 108
easy root, 32
efficiency
BitLocker Drive Encryption, 162
domain controllers, 42, 76
LDAP support, 5
RODC considerations, 107
SMTP support, 207
Enterprise Admins group
Administrator account, 23
Administrators group, 23
establishing forest trusts, 236
functionality, 23
identifying standby operations master, 182
removing additional domain controllers, 89
RODC considerations, 130
staged installations, 119
viewing schema, 159
Enterprise Read-Only Domain Controllers group, 129
ESSENTUTL command, 304
Event ID 1046, 290
Event ID 1168, 290
Event ID 1268, 151
Event ID 1646, 287
Event ID 16645, 177
Event ID 16651, 177–178
Event ID 1668, 155
Event ID 1702, 163
Event ID 1703, 163
Event ID 1704, 163
Event ID 5774, 205
event logs, 219
Event Viewer, 151, 205
explicit trusts, 229, 232
event logs, 219
external trusts
authentication across forest boundaries, 232
creating, 240–244
defined, 229
domainwide authentication, 255
one-way outgoing, 242
selective authentication, 250
two-way, 243–244

fault tolerance, 75
federated forest design, 233
File Replication Service. See FRS (File Replication Service)
File Replication Service log, 219
FileReplicaConn monitoring object, 219
FileReplicaSet monitoring object, 219
firewalls, 208, 267
ForeignSecurityPrincipals container, 49

forest functional levels
defined, 38
features available, 39
levels supported, 20–21, 38–39
RODC considerations, 107
setting, 261–262
Forest Root Domain container, 30
forest root domains
defined, 30
Domain Rename tool, 33
establishing, 32
operations master considerations, 169
PDC emulators, 175
schema masters, 180
Windows Time service, 263, 268
forest schemas, 40
forest trusts
creating, 247–251
defined, 32, 232
establishing, 236
federated forest design, 233
forestwide authentication, 255
selective authentication, 256–257
ForestDNSZones, 106
forests
adding domain trees, 33
as logical components, 16, 20–21
authentication across boundaries, 232–233
creating, 41–59
defining, 20
defining domain hierarchy, 33
domain naming master, 168
establishing infrastructure, 32–34
global catalog servers, 140–141
global catalogs, 34
name suffix routing, 165–166
namespace considerations, 33–34
preparing, 40
removing additional domain controllers, 89
schema master, 168
time synchronization, 264
trust considerations, 34
trusted, 228
trusting, 228
Forward Lookup Zone, 49
FQDN (fully qualified domain name), 6
FRS (File Replication Service)
cleaning up metadata in forests, 102
domain functional levels, 37
replication support, 193
service dependencies, 219
stopping AD DS, 261
SYSVOL replication, 219, 285
full server backups
defined, 278
functionality, 281
scheduling, 208
fully qualified domain name (FQDN), 6
functional levels. See domain functional levels; forest functional levels

garbage collection, 75, 287–288
GET-EVENTLOG command, 305
GET-PROCESS command, 305
gps (Global Positioning System), 264
gps (Global Positioning System), 264
GPUPDATE command, 305
Group object class, 12–13
Group Policy
Configure Windows NTP Client setting, 270–271
CrossSiteSyncFlags setting, 270
EventLogFlags setting, 270
NtpServer setting, 270
ResolvePeerBackOffMaxTimes setting, 270
ResolvePeerBackOffMinutes setting, 271
SpecialPollInterval setting, 271
Type setting, 271
configuring Windows Time settings, 269–277
controlling SRV record registration, 152
Enable Windows NTP Client setting, 269
Enable Windows NTP Server setting, 270
Force Rediscovery Interval Group Policy setting, 206
functionality, 5
Global Configurations Settings policy, 271–277
AnnounceFlags setting, 272
EventLogFlags setting, 272
FrequencyCorrectRate setting, 273
HoldPeriod setting, 273
LargePhaseOffset setting, 273
LocalClockDispersion setting, 274
MaxAllowedPhaseOffset setting, 274
MaxNegPhaseCorrection setting, 274
MaxPollInterval setting, 275
MaxPosPhaseCorrection setting, 275
MinPollInterval setting, 276
PhaseCorrectionRate setting, 276
PollAdjustFactor setting, 276
SpikeWatchPeriod setting, 276
UpdateInterval setting, 277
site considerations, 88
universal group membership
caching, 152–157
global catalogs
deleting, 287
forest considerations, 34
hosting, 168
infrastructure master, 169, 174
LDAP searches, 158
monitoring/verifying promotion, 143–148
removing, 151
replication considerations, 140, 142–143
replication support, 193
RODC support, 106
site considerations, 190
global groups, 153, 229
Global Positioning System (GPS), 264
GPS (Global Positioning System), 264
Group Policy Creator Owners group

Group Policy Creator Owners group, 23
Try Next Closest Site Group Policy setting, 205
Group Policy Creator Owners group, 23, 130
Group Policy Management, 206, 277
group type conversion, 37–38
groups. See specific user groups

H
hard disks
checking for free disk space, 287–288
writable domain controllers, 75
host (A) resource records, 34, 204

I
Include Inheritable Permissions From This Object’s Parent permission, 292
incoming trusts establishing, 236–239
one-way, 238
one-way external, 241
one-way forest, 248
one-way realm, 251
one-way shortcut, 244–245
indexing attributes, 162
inetOrgPerson objects, 39
infrastructure masters functionality, 168
global catalog and, 169
hosting considerations, 174
in domains, 168
locating, 174
managing, 173–175
placement considerations, 171
transferring roles, 169, 174–175
infrastructure, establishing/modifying, 31–36
inheritance, organizational units, 22
installation
AD DS binaries, 41, 74, 76
DNS, 7–8
domain controllers, 42–59, 168, 286
nonstaged, 109
RODC considerations, 107–108, 119–126
staged, 109, 119–126
verifying, 49, 83, 115
writable domain controllers, 75
integrity checks, 290
interforest trusts, 32
InterNIC, 17
intersite replication bandwidth optimization, 194
bridgehead servers, 192, 214
configuring, 206–218
defined, 190–191
designing, 197–200
functionality, 195–197
sistentOwner support, 216
listing time between, 221

K
KCC (Knowledge Consistency Checker) enhancements, 192
Event ID 1268, 151
forest functional levels, 39
functionality, 197
intersite replication, 195–196, 207
locating, 216, 221
site link bridging, 200
Kerberos authentication authentication across forest boundaries, 233
functionality, 5, 230, 232
key distribution center, 36, 38
realm trusts, 236
replication support, 193
service dependencies, 219
time divergence considerations, 263
troubleshooting, 254
trust support, 20
Kerberos Target (krbtgt) account, 10, 106, 130
key distribution center (KDC) domain functional levels, 36
functionality, 230–231

L
LANs (local area networks), 14, 35
LDAP (Lightweight Directory Access Protocol)
  encryption support, 5
  functionality, 5
global catalog searches, 158
performance counters, 219
replication support, 193
service dependencies, 219
LDAP performance counters, 219
Ldp.exe tool, 146, 156–157
leaf objects (leafs), 11
link cost, 208, 212
local area networks (LANs), 14, 35
Local Security Authority (LSA), 195
locking out accounts, 195
logical components
domain trees, 16, 18
domains, 16–18
forests, 16, 20–21
organizational units, 16, 21–22
logon process
account lockouts, 195
authentication considerations, 192, 230
site considerations, 190
updating time stamps, 37–38
UPN support, 230
LSA (Local Security Authority), 195

M
Managed Service Accounts, 39
MAPI (Messaging Application Programming Interface), 5
mapping network structure, 197–198
Maximum Tolerance For Computer Clock Synchronization policy, 263
memberOf attribute, 279
memory requirements, 75
Messaging Application Programming Interface (MAPI), 5
metadata, 97, 102–104
Microsoft Exchange servers, 35, 144, 190
MMC (Microsoft Management Console)
Active Directory Schema tool, 25, 159–161
graphical administration tools, 24
monitoring
global catalogs, 143–148
ISTGs, 216
replication, 144, 218–220
replication attributes, 163
universal group membership
 caching, 155–157
msDS-AuthenticatedToAccountList
 attribute, 128
msDS-NeverRevealGroup attribute, 128
msDS-Preferred-GC-Site attribute, 155
msDS-RevealedUsers attribute, 128
msDS-Reveal-OnDemandGroup
 attribute, 128
multimaster replication model
domain controller support, 9
functionality, 8–9, 191–192
multiple sites, replicating, 192

N
name suffixes
authentication and, 163
configuring routing,
165–166
configuring UPN, 164–165
namespaces
forest considerations, 33–34
site design considerations, 198
nesting groups, 37–38
NET ACCOUNTS command, 306
NET COMPUTER command, 306
NET CONFIG SERVER command,
306
NET CONFIG WORKSTATION com-
mmand, 306
NET CONTINUE command, 307
NET FILE command, 307
NET GROUP command, 307
NET LOCALGROUP command, 307
Net Logon service, 205
NET PAUSE command, 308
NET PRINT command, 308
NET SESSION command, 308
NET SHARE command, 308
NET START command
functionality, 308
starting AD DS, 289, 291, 293
starting W32time service, 269
NET STATISTICS command, 308
NET STOP command
functionality, 309
stopping AD DS, 289, 290–293
stopping W32time service, 269
NET TIME command, 309
NET USE command, 309
NET USER command, 49–52, 309
NET VIEW command, 310
NETDOM ADD command, 310
NETDOM DELETE command, 27, 254–255
NETDOM COMPUTERNAME com-
mmand, 310
NETDOM JOIN command, 311
NETDOM MOVE command, 311
NETDOM MOVENT4BDC command, 311
NETDOM QUERY command
decommissioning domain control-
ners, 89
functionality, 311
identifying operations masters, 169
listing operations masters, 187
NETDOM REMOVE command, 311
NETDOM RENAMECOMPUTER com-
mmand, 312
NETDOM RESET command, 312
NETDOM RESETPWDM command, 312
NETDOM TRUST command, 312
NETDOM VERIFY command, 313
NETSH command, 313
network addresses, 202
network ID, 202
network structure, mapping,
197–198
Network Time Protocol. See NTP
(Network Time Protocol)
New Trust Wizard
establishing trusts, 236–239
one-way incoming external
trusts, 241
one-way incoming forest trusts,
248
one-way incoming realm trusts,
251
one-way incoming shortcut
trusts, 244
one-way outgoing external
trusts, 242
one-way outgoing forest trusts,
249
one-way outgoing realm trusts,
252
one-way outgoing shortcut
trusts, 245
two-way external trusts, 243
two-way forest trusts, 250
two-way realm trusts, 252
two-way shortcut trusts, 246
NLTEST command, 147, 188
nonauthoritative restores, 278,
281–282
nondedicated domain control-
iners, 279
nonstaged installations, 109
NS resource records, 204
NSLOOKUP command, 313
NT LAN Manager (NTLM), 232–233,
282–283
NTDS Settings object, 104, 149
Ntds.dit database file, 141, 280,
286–291
Ntdsutil.exe tool
authoritative restores, 284–285
cleaning up server metadata,
103–104
functionality, 27
listing operations masters, 187
moving directory database,
290–293
offline defragmentation, 289–290
NtFrS (File Replication Service), 219
NTP (Network Time Protocol)
external time sources, 264–265
FrequencyCorrectRate setting, 264
functionality, 263–264
MaxPollInterval setting, 264
MinPollInterval setting, 264
testing communications, 267
UpdateInterval setting, 264

O
object classes, 12, 39
objects
attribute support, 11
common names, 30
connection, 221
container, 11
defined, 11
distinguished names, 30
grouping into logical categories,
30
leaf, 11
lingering, 150
protecting from accidental
deletion, 259–260
restoring with group member-
ships, 279
RODC support, 106
schema support, 12–13
Offline Domain Joins, 39
one-way trusts
defined, 32
incoming, 238
incoming external, 241
incoming forest, 248
incoming realm, 251
incoming shortcut, 244–245
outgoing, 238
outgoing external, 242
outgoing forest, 249
outgoing realm, 252
outgoing shortcut, 245–246
operations masters. See also PDC
emulators
assigning, 174
availability by category, 168
changing, 170–171
cleaning up old references, 286
decommissioning, 183
defined, 167
domain controllers, 74, 89
domain naming masters, 168, 170,
172–173
identifying, 169
improper placement, 169–170
infrastructure masters, 168–169,
171, 173–175
planning for, 169–170
reducing workload, 183–185
RID masters, 168–169, 171,
177–179, 195
RODC considerations, 106
schema masters, 168, 170,
180–181
seizing roles, 170, 185–187
standby, 168, 181–182
transferring roles, 170
troubleshooting, 187–188
organizational domains, 6
organizational units (OUs)
as logical components,
16, 21–22
cleaning up server metadata, 102
defined, 21
establishing infrastructure, 34
inheritance, 22
outgoing trusts
establishing, 236–239
one-way, 238

327
parent domains

one-way external, 242
one-way forest, 249
one-way realm, 252
one-way shortcut, 245–246

P

parent domains, 7, 232
PAS (partial attribute set)
adding attributes, 163
changing, 163
defined, 158
Password Replication Policy
allowing/denying accounts,
130–132
attributes, 128
configuring, 127, 129
deleagating administrative permis-
sions, 135
denial, 130–132
identifying allowed/denied ac-
counts, 133
managing credentials, 106,
132–133
resetting credentials, 134
RODCs, 10, 106, 108, 116
setting, 127–135
passwords
computer accounts, 278, 282
Directory Services Restore Mode,
116
nonpriority changes, 195
PDC emulators, 175
priority replication, 195
RODC considerations, 106, 108,
128–129
trust, 237
PATHPING command, 313
PDC emulators
configuring, 218–219
performance counters
changing passwords, 195
cleaning up old references, 286
forest functional levels, 21
functionality, 168
in domains, 168
locating, 176
managing, 175–177
placement considerations, 171
reducing workloads, 183
RODC considerations, 107
time synchronization, 264, 268
transferring roles,
169, 176–177
verifying trusts, 254
performance counters
AB, 218
ATQ, 218
DRA, 219
DS, 219
functionality, 218–219
LDAP, 219
SAM, 219
Performance Monitor, 218–219
permissions
Allowed To Authenticate permis-
sion, 256–257
deleagating, 135
Deny Delete Subtree permission, 259
Include Inheritable Permissions
From This Object’s Parent
permission, 292
trusts and, 228
physical components
defined, 14
sites, 14–16, 35
subnets, 14–16
PING command, 313
prefix notation, 202
primary domain controllers. See PDC
emulators
Printer object class, 12–13
Printer objects, 11
Printers object, 11
privileges, trusts and, 228
pull replication, 194
push replication, 194
monitoring replication process,
144, 220
removing lingering objects, 150
synchronizing replication, 223
troubleshooting operations
masters, 188
REPL interface, 5, 158
replication. See also intersite replica-
tion; intrasite replication
adding RODCs using, 109–115
adding writable domain control-
liers using, 76–83
bandwidth and, 191
domain controller support, 21
esential services, 193–194
generating topology, 222
global catalogs, 140, 142–143
listing failed events, 221
listing queued tasks, 221
listing state summary, 221
monitoring process, 144, 218–220
multmaster, 8–9, 191–192
multiple sites, 192
priority, 195
pull, 194
push, 194
REPL interface, 5, 158
RODC considerations, 107
single-master, 9
site considerations, 16, 190–191
synchronizing, 223
SYSSOL, 193
traffic compression, 190, 192, 195
troubleshooting, 219–221
verifying and forcing, 222–223
replication attributes
changing, 160–162
default, 158
designating, 159–162
monitoring, 163
troubleshooting, 163
replication interval, 208
replication properties, 207
replication schedules
configuring, 210–212
scheduling traffic, 192
site links, 208
resource records, 34. See also spec-
cific resource records
resources. See also objects
DNS support, 6
site boundary considerations, 191
site design considerations, 198
trust considerations, 228–229
restore procedures. See backup and
restore procedures
Resultant Set of Policy, 133
Revealed Accounts list, 128
Reverse Lookup Zone, 49
RID (relative ID) masters
functionality, 168
in domains, 168
locating, 178
managing, 177–179
placement considerations, 171
priority replication, 195
transferring roles, 169, 179
RID pool, 177
ring topology, 194
RODCs (read-only domain controllers)
adding to domains, 108–119
adding using answer files/command line, 115–119
adding using replication, 109–115
attaching, 121–122, 125–126
creating account, 120–121, 123–125
decommissioning, 126–127
defined, 10
deploying, 39
establishing infrastructure, 36
functionality, 10
identifying allowed/denied accounts, 133
installing, 107
installing from media, 108
managing credentials, 106, 132–133
PDC emulators, 175
preparing, 40
preparing for deployment, 106–108
setting Password Replication Policy, 127–135
staged installations, 119–126
role-based authorization, 39
root domains. See also forest root domains
defined, 6
domain trees, 18
TLD, 6–7
rootDSE
containers below, 30
defined, 30
global catalog searches, 158
isGlobalCatalogReady attribute, 145
updateCachedMemberships attribute, 156–157
ROUTE command, 314
RPC (remote procedure call)
domain naming masters, 172
intrasite replication, 194, 221
replication support, 193
service dependencies, 219
site link support, 207
RPC over IP
replication support, 194, 196
site link support, 207
SC START command, 315
SC STOP command, 315
scheduling
full server backups, 208
replication, 192, 208, 210–212
schema
defined, 12
domain controllers, 34
extending, 13
functionality, 11–13
viewing, 159
Schema Admins group
Active Directory Schema tool, 160, 180
Administrator account, 23
functionality, 23
RODC considerations, 130
schema attribute objects (schema attributes), 12–13
schema class objects (schema classes), 12–13
Schema container, 30, 180
schema masters
domain controllers, 168
functionality, 168
in forests, 168
locating, 180
managing, 180–181
placement considerations, 170
replicating changes, 191
RODC considerations, 130
schema objects, 12
schema partitions
bridgehead servers, 214
domain controllers, 31
replicating changes, 191
SCHTASKS /CHANGE command, 315
SCHTASKS /CREATE command, 316
SCHTASKS /DELETE command, 316
SCHTASKS /END command, 316
SCHTASKS /QUERY command, 316
SCHTASKS /RUN command, 316
searchFlags property, 162
Secure Sockets Layer (SSL), 158, 193
Security Accounts Manager interface. See SAM (Security Accounts Manager) interface
security identifiers. See SIDs (security identifiers)
security principals
domain functional level support, 37–38
RID masters, 177
security tokens, 229
selective authentication configuring, 255–257
defined, 239
for external trusts, 256
for forest trusts, 256–257
Server Manager
Add Feature Wizard, 24, 277
Add Role feature, 41
starting/stopping AD DS, 260–261
Server Message Block (SMB), 193
server objects, 104
SERVERMANAGERCMD command
adding RODCs, 109
functionality, 316
installing AD DS binaries, 41, 76
service principal name (SPN), 165
session key, 231
session ticket, 231
SET command, 231
SET-SERVICE command, 317
shortcut trusts
creating, 244–247
defined, 229
SHUTDOWN command, 317
SIDs (security identifiers)
authentication process, 140, 152–153
RID support, 168, 177
Simple Mail Transfer Protocol. See SMTP (Simple Mail Transfer Protocol)
site design
associating subnets to sites, 197
designing intersite replication, 197–200
designing sites, 197
devolving, 197–200
mapping network structure, 197–198
planning server placement, 197, 200
site link bridges, 197, 199, 212–213
site link cost, 208, 212
site links
availability, 210
cache refresh considerations, 156
configuring, 35, 206–218
creating, 208–209
default, 206
functionality, 206–208
intersite replication, 196
link cost, 208, 212
optimizing configurations, 217–218
replication interval, 208
replication schedules, 208, 210–212
RODC support, 36
setting site boundaries, 190
site design considerations, 197
WAN considerations, 36, 190
sites
adding domain controllers, 203–205
as physical components, 14–16, 35
associating subnets, 197–198, 201–202
bridging, 212–213
configuring, 200–206
controlling SRV record registration, 152
creating, 200–201
default, 200
defined, 14, 189
designing, 197–198
domain controllers, 16, 35, 74
domains spanning, 18
establishing infrastructure, 35–36
functionality, 14, 190
global catalog servers, 88, 142
mapping network structure, 197–198
mapping subnets, 15
locating ISTGs, 216
moving domain controllers, 202
object support, 16
replicating multiple, 192
RODC considerations, 107
setting boundaries, 190–191
SMB (Server Message Block), 193
SMTP (Simple Mail Transfer Protocol) replication support, 194, 196 site link support, 207–208, 210 SMTP Server feature, 207 SPN (service principal name), 165 SRV resource records cleaning up old references, 286 controlling registration, 152 DNS server considerations, 34, 183 domain name values, 148 host server values, 148 NETLOGON errors, 205 port number values, 148 priority values, 148–149, 184–185 protocol values, 148 service values, 148 verifying global catalog servers, 147–148 weight values, 148–149, 183–185 SSL (Secure Sockets Layer), 158, 193 staged installations attaching RODC, 121–122, 125–126 creating RODC account, 120–121 RODC considerations, 109, 119 using command line/answer files, 123–126 standby operations masters, 168, 181–182 static IP addresses, 34, 41 STOP-PROCESS command, 318 STOP-SERVICE command, 318 storage considerations, 7, 75 stored policies, 37 subdomains, 7 subnets adding domain controllers to sites, 203 as physical components, 14–16 associating to sites, 197–198, 201–202 configuring, 200–206 creating, 200, 202 defined, 14, 189 functionality, 14–16 grouping into sites, 15 IP addresses, 14, 200, 202 site design considerations, 197–198 well connected, 15 synchronizing computer time, 263–277 directory partitions, 163 replication, 223 System Configuration tool, 98–99 System log NETLOGON errors, 205 W32time errors, 267 system state backups considerations, 287 defined, 278 functionality, 280–281 SYSTEMINFO command, 318 SYSVOL data DFS support, 37–38, 219 FRS support, 37, 219 replication considerations, 193

restoring, 285–286 RID pools, 177 service dependencies, 219

T

U

V

W
W32tm tool config parameter, 266, 268–269 dataonly parameter, 265 manualpeerlist parameter, 266, 268–269 monitor parameter, 265
nowait parameter, 265
query parameter, 266
rediscove parameter, 265
register parameter, 265, 269
reliable parameter, 266, 268
ressync parameter, 265
stripchart parameter, 265, 267–268
syncfromflags parameter, 266, 268–269
threads parameter, 265
unregister parameter, 265, 269
update parameter, 266, 268
WAN (wide area network), 36, 190
Wbadmin tool
accessing, 277
backup support, 278
functionality, 319–320
Start SystemStateBackup com-
mand, 280
Start SystemStateRecovery com-
mand, 280–281
well connected subnets, 15
wide area network (WAN), 36, 190
Windows 2000
domain functional levels, 36
forest functional levels, 20, 38
RODC support, 106
SYSVOL replication, 193
verifying trusts, 254
Windows 2000 Server, 260
Windows Firewall, 26
Windows NT
SAM limitations, 8
trust considerations, 229, 232, 254
Windows Server 2003
domain functional levels, 36
forest functional levels, 20, 38
KCC enhancements, 192
RODC support, 106
stopping AD DS, 260
SYSVOL replication, 193
Windows Server 2008
deploying, 40–41
domain functional levels, 36
forest functional levels, 21, 38-39
KCC enhancements, 192
Protect Object From Accidental
Deletion option, 259
RODC support, 106
SYSVOL replication, 193
Windows Server 2008 R2 forest
functional level, 21, 26, 39
Windows Server Backup, 277
Windows Time service (W32time)
checking configuration, 266–267
configuring settings, 265–266,
269–277
configuring time source, 268
functionality, 175, 264
restoring default settings, 269
time divergence considerations, 263
troubleshooting, 269
Windows Vista
RODC support, 106
time synchronization, 264
Windows XP
RODC support, 106
time synchronization, 264
writable domain controllers
adding using answer files/com-
mand line, 85–87
adding using replication, 76–83
hard disk requirements, 75
installing additional, 75
memory requirements, 75

Z
zone, 7
zone transfers, 7
About the Author

William R. Stanek (http://www.williamstanek.com/) was born in Burlington, Wisconsin, where he attended public schools, including Janes Elementary School in Racine, Wisconsin. He is the second youngest of five children. After a career in the military, he settled in Washington State, having been captivated by the rugged beauty of the Pacific Northwest.

In 1985 he enlisted in the U.S. Air Force and entered a two-year training program in intelligence and linguistics at the Defense Language Institute. After graduation he served in various field operations duties in Asia and Europe. In 1990 he won an appointment to Air Combat School and shortly after graduation served in the Persian Gulf War as a combat crewmember on an electronic warfare aircraft. During his two tours in the Persian Gulf War, William flew numerous combat and combat support missions, logging over 200 combat flight hours. His distinguished accomplishments during the war earned him nine medals, including the United States of America’s highest flying honor, the Air Force Distinguished Flying Cross, as well as the Air Medal, the Air Force Commendation Medal, and the Humanitarian Service Medal. He earned 29 decorations in his military career.

In 1994 William earned his bachelor’s degree magna cum laude from Hawaii Pacific University. In 1995 he earned his master’s degree with distinction from Hawaii Pacific University. In 1996 he separated from the military, having spent 11 years in the U.S. Air Force. While in the military, he was stationed in Texas, Japan, Germany, and Hawaii. He served in support of Operation Desert Storm, Operation Desert Shield, and Operation Provide Comfort. His last station while in the Air Force was with the 324th Intelligence Squadron, Wheeler Army Airfield, Hawaii.

Born into a family of readers, William was always reading and creating stories. Even before he started school, he read classics like Treasure Island, The Swiss Family Robinson, Kidnapped, Robinson Crusoe, and The Three Musketeers. Later in his childhood, he started reading works by Jules Verne, Sir Arthur Conan Doyle, Edgar Rice Burroughs, Ray Bradbury, Herman Melville, Jack London, Charles Dickens, and Edgar Allan Poe. Of that he says, “Edgar Allan Poe can be pretty bleak and dark, especially when you’re 10 years old. But I remember being fascinated with his stories. To this day I can still remember parts of ‘The Raven,’ The Tell Tale Heart, and The Murders in the Rue Morgue.”

William completed his first novel in 1986 when he was stationed in Japan, but it wasn’t until nearly a decade later that his first book was published. Since then, he has written and published nearly 100 books, including Active Directory Administrator’s Pocket Consultant, Windows Server 2008 Administrator’s Pocket Consultant, SQL Server 2008 Administrator’s Pocket Consultant, and Windows Server 2008 Inside Out (all from Microsoft Press).
In 1997, William was dubbed “A Face Behind the Future” in a feature article about his life in The (Wash.) Olympian. At that time he was breaking new ground in shaping the future of business on the Internet. Today William continues to help shape the future of Internet business and technology in general, writing authoritative books covering these subjects for a variety of publishers. William has won many awards from his colleagues and the publishing industry.

For fun he used to spend a lot of time mountain biking and hiking, but now his adventures in the great outdoors are mostly restricted to short treks around the Pacific Northwest. In 2009, William’s one-hundredth book will be published by Microsoft. William’s life-long commitment to the printed word has helped him become one of the leading technology authors in the world today.