



Windows Server® 2008

Portable Command Guide

All the MCTS 70-640, 70-642, 70-643,
and MCITP 70-646, 70-647 Commands
in One Compact, Portable Resource

PEARSON

DARRIL GIBSON

**Windows Server 2008 Portable
Command Guide: MCTS 70-640, 70-642,
70-643, and MCITP 70-646, 70-647**

Darril Gibson

Pearson Education
800 East 96th Street
Indianapolis, Indiana
46240
USA

Windows Server 2008 Portable Command Guide: MCTS 70-640, 70-642, 70-643, and MCITP 70-646, 70-647

Copyright © 2011 by Pearson Education, Inc.

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

ISBN-13: 978-0-7897-4737-2

ISBN-10: 0-7897-4737-5

Library of Congress Cataloging-in-Publication data is on file.

Printed in the United States of America

First Printing: May 2011

Trademarks

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

Warning and Disclaimer

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

Bulk Sales

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

U.S. Corporate and Government Sales

1-800-382-3419

corpsales@pearsontechgroup.com

For sales outside the United States, please contact

International Sales

international@pearson.com

Associate Publisher

Dave Dusthimer

Acquisitions Editor

Betsy Brown

Development Editor

Jeff Riley

Series Editor

Scott Empson

Managing Editor

Sandra Schroeder

Senior Project Editor

Tonya Simpson

Copy Editor

Deadline Driven
Publishing

Proofreader

Leslie Joseph

Technical Editor

David Camardella

Publishing Coordinator

Vanessa Evans

Book Designer

Gary Adair

Composition

Bronkella Publishing

Contents at a Glance

Introduction xvii

PART I: Command Prompt Basics

- CHAPTER 1** Launching and Using the Command Prompt 1
- CHAPTER 2** Basic Rules When Using the Command Prompt 9
- CHAPTER 3** Manipulating Files, Folders, and Shares 21
- CHAPTER 4** Creating Batch Files 37

Part II: Managing and Troubleshooting DNS

- CHAPTER 5** Using **dnscmd** 47
- CHAPTER 6** Using **nslookup** 55

Part III: Managing and Troubleshooting Active Directory

- CHAPTER 7** Using Basic **ds** Commands 63
- CHAPTER 8** Using Advanced **ds** Commands 71
- CHAPTER 9** Promoting and Demoting a Domain Controller (DC) 77
- CHAPTER 10** Working with the Schema 87
- CHAPTER 11** Working with Active Directory Accounts 91
- CHAPTER 12** Using **ntdsutil** 101
- CHAPTER 13** Using **netdom** 111
- CHAPTER 14** Troubleshooting Replication 119

Part IV: Group Policy and the Command Line

- CHAPTER 15** Group Policy Overview 127
- CHAPTER 16** Group Policy Command-Line Tools 143
- CHAPTER 17** Security Configuration Wizard 149

Part V: Configuring Server Core

- CHAPTER 18** Configuring Server Core after Installation 155
- CHAPTER 19** Adding Roles to Server Core 163
- CHAPTER 20** Configuring Server Core for Remote Administration 171

Part VI: Managing and Maintaining Windows Server 2008 and Windows Server 2008 R2

- CHAPTER 21** Manipulating Services 177
- CHAPTER 22** Basic Routing on a Server 187
- CHAPTER 23** Working with Printers 193
- CHAPTER 24** Licensing and Activation 201
- CHAPTER 25** Using **netsh** 209
- CHAPTER 26** Working with Event Subscriptions 219
- CHAPTER 27** Using **wbadmin** 231

Part VII: Troubleshooting Windows Server 2008 and Windows Server 2008 R2

- CHAPTER 28** Troubleshooting Networking Issues 241
- CHAPTER 29** Using the Reliability and Performance Monitor 253
- CHAPTER 30** Using Network Monitor and **nmcap** 261

Part VIII: Terminal Services and Remote Desktop Services

- CHAPTER 31** Remote Desktop Services 269
- CHAPTER 32** Remote Administration 277

Part IX: Working with Some Server Roles from the Command Line

- CHAPTER 33** Using Windows Deployment Services 283
- CHAPTER 34** Manipulating IIS with **appcmd** 293

Part X: Using Visual Basic Scripts (VB Script)

- CHAPTER 35** Creating Basic Visual Basic Scripts 297
- CHAPTER 36** Manipulating Active Directory with Visual Basic Scripts 305

Part XI: Using PowerShell

- CHAPTER 37** Starting and Using PowerShell 311
- CHAPTER 38** Creating and Running a PowerShell Script 331
- CHAPTER 39** Using the Integrated Scripting Environment 347
- CHAPTER 40** Using PowerShell to Manage Active Directory 357
- APPENDIX** Create Your Own Journal Here 365

Table of Contents

Introduction xvii

Part I: Command Prompt Basics

CHAPTER 1	Launching and Using the Command Prompt	1
	Launching the Command Prompt	1
	Launching with Elevated Privileges	2
	Using the Built-in doskey Program	3
	Creating Mini Macros with doskey	5
	Cutting and Pasting to and from the Command Prompt	5
	Copying from the Command Prompt Window	6
	Pasting Data to the Command Prompt Window	6
	Changing the Options and Display	7
CHAPTER 2	Basic Rules When Using the Command Prompt	9
	Using Uppercase or Lowercase	9
	Using Quotes	10
	Understanding Variables	11
	Understanding Switches	13
	Understanding Wildcards	13
	Getting Help	14
	Understanding Paths	17
	Using Basic Commands	18
	Redirecting Output to Files	19
CHAPTER 3	Manipulating Files, Folders, and Shares	21
	Copying Files with copy, xcopy, and robocopy	21
	copy	21
	xcopy	22
	robocopy	23
	Compressing Files with compact	26
	Encrypting Files with cipher	27
	Manipulating Shadow Copies with vssadmin	28
	Manipulating Shares with net share	31
	Mapping Drives with net use	32

Manipulating Users and Groups with the net Command 33
Modifying NTFS Permissions with icacls 34

CHAPTER 4 Creating Batch Files 37
Using Notepad 37
Giving Feedback with echo 38
Using Parameters 39
Calling Another Batch File with call 41
Clearing the Screen with cls 42
Changing the Order of Processing with goto 42
Checking Conditions with if 43

Part II: Managing and Troubleshooting DNS

CHAPTER 5 Using dnscmd 47
Retrieving DNS Information 47
Exporting DNS Data 49
Forcing Zone Transfers 49
Clearing the DNS Cache 49
Working with DNS Partitions 50
Adding DNS Zones 51
Creating and Deleting DNS Records 53

CHAPTER 6 Using nslookup 55
Verifying Records with nslookup 55
Configuring DNS for nslookup 58
Using nslookup Without PTR Records 59
Using nslookup Without a Reverse Lookup Zone 60

Part III: Managing and Troubleshooting Active Directory

CHAPTER 7 Using Basic ds Commands 63
Understanding Distinguished Names 63
Adding Objects with dsadd 65
Modifying Accounts with dsmod 67
Moving Accounts with dsmove 69
Removing Objects with dsrm 70

- CHAPTER 8** Using Advanced ds Commands 71
- Retrieving Information about Objects with dsquery 71
 - Retrieving Information About Objects with dsget 73
 - Viewing and Modifying AD Permissions with dscls 75
- CHAPTER 9** Promoting and Demoting a Domain Controller (DC) 77
- Promoting a DC with dcpromo 77
 - Demoting a DC with dcpromo 79
 - Using dcpromo with an unattend File 80
 - Promoting a DC to an RODC with an Existing Account 81
 - Using dcpromo to Install from Media 83
 - Forcing Removal of Active Directory 84
- CHAPTER 10** Working with the Schema 87
- Modifying the Schema with adprep 87
 - Registering the Active Directory Schema Snap-In 88
- CHAPTER 11** Working with Active Directory Accounts 91
- Using ldifde to Export, Import, and Delete Accounts 91
 - Using csvde to Export and Import Accounts 95
 - Redirecting Computer Accounts 97
 - Redirecting User Accounts 98
- CHAPTER 12** Using ntdsutil 101
- Resetting the Directory Services Restore Mode Password 101
 - Changing the Garbage Collection Logging Level 102
 - Moving Active Directory to a Different Drive 103
 - Defragmenting Active Directory 104
 - Performing an Authoritative Restore 105
 - Removing a Domain Controller from Active Directory 107
 - Seizing an Operations Master Role 108
- CHAPTER 13** Using netdom 111
- Identifying Operations Master Roles 111
 - Joining a Computer to a Domain 111
 - Verifying Trust Relationships 113
 - Querying and Resetting Secure Channels with netdom 116

- CHAPTER 14** Troubleshooting Replication 119
 - Checking Replication with repadmin 119
 - Forcing Replication with repadmin 121
 - Migrating to DFSR with dfsrmig 123

Part IV: Group Policy and the Command Line

- CHAPTER 15** Group Policy Overview 127
 - Launching the Group Policy Management Console 127
 - Understanding Group Policy Order of Precedence 128
 - Filtering GPOs by Modifying Permissions 130
 - Understanding Group Policy Settings 132
 - Enabling Auditing Through Group Policy 132
 - Enabling Advanced Auditing for Directory Services Changes 134
 - Deploying Applications 135
 - Configuring Automatic Updates 137
 - Blocking Inheritance 138
 - Enforcing GPOs 138
 - Using Loopback Processing 139
 - Running Scripts with Group Policy 140
- CHAPTER 16** Group Policy Command-Line Tools 143
 - Viewing Group Policy Settings with gpresult 143
 - Refreshing Group Policy Settings with gpupdate 146
- CHAPTER 17** Security Configuration Wizard 149
 - Understanding the Security Configuration Wizard 149
 - Using scwcmd 151

Part V: Configuring Server Core

- CHAPTER 18** Configuring Server Core after Installation 155
 - Installing Server Core 155
 - Restoring the Command Prompt 156
 - Renaming the Computer 157
 - Logging Off, Shutting Down, and Rebooting 158
 - Configuring TCP/IP 159
 - Setting the Time, Date, and Time Zone 160
 - Joining a Domain 161

CHAPTER 19	Adding Roles to Server Core	163
	Understanding the Supported Roles	163
	Using ocsetup to Add Roles to Windows Server 2008	164
	Adding the DHCP Server Role with ocsetup	165
	Adding the DNS Server Role with ocsetup	166
	Adding File Services with ocsetup	166
	Adding the Print Services Role with ocsetup	166
	Adding the Web Server (IIS) Role with pkgmgr	166
	Using dism to Add Roles to Windows Server 2008 R2	167
	Adding the DHCP Server Role with dism	168
	Adding the DNS Server Role with dism	168
	Adding File Services with dism	169
	Adding the Print and Document Services Role with dism	169
	Adding the AD CS Role with dism	169
	Adding the AD LDS Role with dism	169
	Adding PowerShell with dism	170
	Adding the AD DS Role	170
CHAPTER 20	Configuring Server Core for Remote Administration	171
	Using the Server Core Registry Editor	171
	Enabling Access with Remote Microsoft Management Consoles (MMCs)	173
	Configuring the Firewall to Reply to Ping	175
Part VI: Managing and Maintaining Windows Server 2008 and Windows Server 2008 R2		
CHAPTER 21	Manipulating Services	177
	Stopping and Starting Services with the net Command	177
	Manipulating Services with sc	178
	Manipulating Services with wmic	181
	Configuring the Firewall to Allow wmic	181
	Using the wmic service list Command	182
	Using the wmic service call Command	183
CHAPTER 22	Basic Routing on a Server	187
	Viewing the Routing Table with route print	187
	Adding Routes to the Routing Table with route add	189
	Modifying Routes in the Routing Table with route change	191
	Deleting Routes from the Routing Table with route delete	192

CHAPTER 23	Working with Printers	193
	Publishing Printers to Active Directory with pubprn.vbs	193
	Migrating Printers with printbrm	196
	Controlling the Print Queue with prnqctl.vbs	197
CHAPTER 24	Licensing and Activation	201
	Managing Activation Tasks with slmgr	201
	Managing Basic Tasks with slmgr	201
	Viewing License Information with slmgr	202
	Managing KMS Servers with slmgr	203
	Using KMS Activation Keys	204
	Managing KMS Clients with slmgr	204
	Forcing Registration of KMS Server SRV Records	205
	Manually Creating an SRV Record for KMS	206
CHAPTER 25	Using netsh	209
	Understanding netsh	209
	Understanding netsh Contexts	210
	Configuring IPv4 with netsh	214
	Configuring an IPv6 Address with netsh	217
	Disabling IPv6 in Windows Server 2008	218
CHAPTER 26	Working with Event Subscriptions	219
	Enabling the Source Computer with winrm	219
	Enabling the Collector Computer with wecutil	220
	Adding an Account to the Event Log Readers Group	221
	Enabling and Testing Event Subscriptions	223
	Managing Subscriptions with wecutil	226
	Logging Events with eventcreate	228
CHAPTER 27	Using wbadmin	231
	Adding wbadmin to a Server	231
	Backing Up System State Data with wbadmin	232
	Restoring System State Data with wbadmin	233
	Restoring System State Data on a Domain Controller with wbadmin	235
	Backing Up Volumes with wbadmin	236
	Restoring Volumes with wbadmin	238

Part VII: Troubleshooting Windows Server 2008 and Windows Server 2008 R2

- CHAPTER 28** Troubleshooting Networking Issues 241
- Viewing and Manipulating TCP/IP Configuration with ipconfig 241
 - Checking Connectivity with ping 247
 - Viewing the Router Path with tracert 251
 - Checking for Data Loss with pathping 251
- CHAPTER 29** Using the Reliability and Performance Monitor 253
- Gathering Information from the Reliability Monitor 253
 - Running System Data Collector Sets 256
 - Writing a Script to Run Data Collector Sets 258
 - Scheduling a Script to Run Data Collector Sets 259
- CHAPTER 30** Using Network Monitor and nmcap 261
- Installing Network Monitor 261
 - Starting and Using Network Monitor 262
 - Using nmcap to Capture Traffic 264
 - Automatically Starting, Stopping, and Terminating nmcap 265
 - Adding Filters to nmcap 267
 - Enabling Promiscuous Mode in nmcap 268

Part VIII: Terminal Services and Remote Desktop Services

- CHAPTER 31** Remote Desktop Services 269
- Adding the Remote Desktop Services Role 269
 - Viewing and Manipulating the Install Mode with change user 272
 - Modifying Logon Capabilities with change logon 272
 - Connecting and Disconnecting Sessions with tscn and tsdiscon 273
 - Identifying Open Sessions with query user or quser 274
 - Resetting Sessions with reset session 275
- CHAPTER 32** Remote Administration 277
- Configuring, Verifying, and Removing winrm 277
 - Using winrs to Issue Commands 278
 - Connecting to Remote Systems with mstsc 280

Part IX: Working with Some Server Roles from the Command Line

CHAPTER 33 Using Windows Deployment Services 283

- Adding the WDS Role 283
- Configuring the WDS Role 285
- Adding Boot Images to WDS with wdsutil 285
- Creating Image Groups Using wdsutil 286
- Adding Install Images Using wdsutil 286
- Configuring Server Properties Using wdsutil 288
- Running the sysprep GUI 290
- Running sysprep from the Command Line 291

CHAPTER 34 Manipulating IIS with appcmd 293

- Managing Sites with appcmd 293
- Adding a Site with appcmd 294
- Adding an Application to a Site with add app 295
- Adding a Virtual Directory with add vdir 295
- Starting and Stopping Application Pools with appcmd and appcmd stop 296

Part X: Using Visual Basic Scripts (VB Script)

CHAPTER 35 Creating Basic Visual Basic Scripts 297

- Working with filesystemobject 297
- Accessing a Network Share with filesystemobject 300
- Calling Scripts from a Batch File 300
- Displaying a Message Box with a Visual Basic Script 300
- Using if Statements 302
- Checking for a Value with a Message Box 302

CHAPTER 36 Manipulating Active Directory with Visual Basic Scripts 305

- Connecting to Active Directory with a VB Script 305
- Creating an OU with a VB Script 305
- Creating a User Account with a VB Script 306
- Modifying the Tombstone Lifetime 307

Part XI: Using PowerShell

CHAPTER 37 Starting and Using PowerShell 311

- Installing and Launching PowerShell 311
- Understanding PowerShell Verbs and Nouns 312

Tabbing Through PowerShell Commands	316
Understanding the Different Types of PowerShell Commands	318
Creating Aliases	318
Discovering Windows PowerShell Commands	318
Exploring get-member	320
Redirecting Output with Windows PowerShell	322
Understanding PowerShell Errors	323
Understanding PowerShell Variables	324
Using Comparison Operators	327
Understanding Pipelining	327
CHAPTER 38 Creating and Running a PowerShell Script	331
Setting the Security Context	331
Creating a PowerShell Profile	332
Creating and Modifying the Global PowerShell Profile	334
Running PowerShell Scripts	336
Logging Processes with a get-process Script	337
Testing for the Existence of a File	338
Creating Output as HTML	340
Running a Script Against Multiple Computers	341
Scheduling PowerShell Scripts	344
CHAPTER 39 Using the Integrated Scripting Environment	347
Launching the ISE	347
Exploring the ISE	348
Executing Commands in the ISE	350
Creating and Saving a Script in the ISE	351
CHAPTER 40 Using PowerShell to Manage Active Directory	357
Using the Active Directory Module in Windows Server 2008 R2	357
Creating and Manipulating Objects in Windows Server 2008	359
Creating an OU with PowerShell	359
Creating a User with PowerShell	359
Moving Objects with PowerShell	360
Working with the Domain Object	361
Working with the system.directoryservices Namespace	362
Creating a List of Domain Computers	363
APPENDIX Create Your Own Journal Here	365

About the Author

Darril Gibson is the CEO of Security Consulting and Training, LLC. He regularly teaches, writes, and consults on a wide variety of security and technical topics. He has been a Microsoft Certified Trainer since 1999 and holds several certifications, including MCSE (NT 4.0, 2000, 2003), MCDBA (SQL Server), MCITP (Windows 7, Server 2008, and SQL Server), ITIL v3, Security+, and CISSP. He has authored, coauthored, or contributed to more than a dozen books. You can view a listing of most of his current books on Amazon at <http://amzn.to/bL0Obo>.

About the Series Editor

Scott Empson is the associate chair of the Bachelor of Applied Information Systems Technology degree program at the Northern Alberta Institute of Technology in Edmonton, Alberta, Canada, where he teaches Cisco routing, switching, and network design courses. Scott is also the program coordinator of the Cisco Networking Academy Program at NAIT, a Regional Academy covering Central and Northern Alberta. He has earned three undergraduate degrees: a Bachelor of Arts, with a major in English; a Bachelor of Education, again with a major in English/Language Arts; and a Bachelor of Applied Information Systems Technology, with a major in Network Management. Scott also has a Masters of Education degree from the University of Portland. He holds several industry certifications, including CCNP, CCAI, Network+, and CIEH.

Scott is the series creator and one of the authors of the Portable Command Guide Series. Portable Command Guides are filled with valuable, easy-to-access information to quickly refresh your memory. Each guide is portable enough for use whether you're in the server room or the equipment closet.

About the Technical Editor

David Camardella has more than 10 years of experience in networking, including providing technical support and services such as designing and maintaining Cisco Internetworks, Active Directory, messaging infrastructures, and desktop deployment systems. Over the years, David has performed technical editing on several Cisco and Microsoft books. He holds a Bachelor of Science in Business Management as well as several levels of IT certifications, including the MCITP Enterprise Admin/Server Admin Certifications.

Dedication

To my wife, who continues to provide me with love and encouragement. I'm thankful we are sharing our lives together.

Acknowledgments

I'm grateful for all the hard work done behind the scenes by the people at Pearson. I'm thankful to Scott Empson, who had the original vision for these books, and I'm grateful that David Dusthimer had faith in me to head up many of the books in the Microsoft series. I especially appreciated the efforts of the editors: Jeff Riley, David Camardella, Ginny Bess, and Tonya Simpson. This book is much better due to their efforts.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

As an associate publisher for Pearson IT Certification, I welcome your comments. You can email or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

When you write, please be sure to include this book's title and author as well as your name, email address, and phone number. I will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: David Dusthimer
 Associate Publisher
 Pearson IT Certification
 800 East 96th Street
 Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at pearsonitcertification.com for convenient access to any updates, downloads, or errata that might be available for this book.

Introduction

Thanks for buying the *Windows Server 2008 Portable Command Guide: MCTS 70-640, 70-642, 70-643, and MCITP 70-646, 70-647*. I'd love to say that this book was my idea, but the real credit goes to Scott Empson who originally developed the vision of this book with Cisco certifications. I've worked with Scott and Pearson Education to help bring the same type of books he created for Cisco products to professionals working on Microsoft products. Scott's vision started with the idea that many IT professionals who have already learned the theory still sometimes need help remembering how to implement it.

The book doesn't go into depth teaching these concepts. The idea is that you already understand them. Instead, the goal is to provide enough information to help you remember what you can do and how to do it. The book is purposely written to be a small, portable, and useful journal, not an encyclopedic-sized volume. However, even if a concept is new to you, there's enough information for you to start typing at the command prompt to gain a better understanding.

As an example, you probably know that you can force the registration of SRV records in DNS by stopping and restarting a specific service. However, you might not remember the specific commands are **net stop netlogon** and **net start netlogon**. You might remember that you have to join a Server Core computer to a domain using the **netdom** command, but you might not remember the full syntax off the top of your head. In other words, you know the theory behind why you'd stop and restart the netlogon service and why you have to join a Server Core computer to a domain from the command prompt, but you might not always remember the syntax. This book is a ready reference of useful commands and procedures with clear-cut examples. It shows the exact syntax of many of the commands needed for administrative tasks performed regularly by Windows Server 2008 (and Windows Server 2008 R2) administrators.

I started the outline of this book by ensuring that command prompt commands covered by the Microsoft Certified Information Technology Professional (MCITP) certifications on Windows Server 2008 were included. This includes the 70-640, 70-642, 70-643, 70-646, and 70-647 exams for the MCITP Server Administrator and MCITP: Enterprise Administrator certifications. I then added the commands I've found valuable in my day-to-day work on networks and from classroom teaching.

Many IT professionals use an engineering journal to help them remember key information needed on the job. It might include specific commands that they sometimes forget, IP addressing schemes used on their networks, steps for important maintenance tasks that are performed infrequently, or anything else they want to easily recall by looking at the journal. If you already have an engineering journal of your own, you can add this as a Windows Server 2008 addendum. If you don't have one, you can start with this book. It includes the same "Create Your Own Journal Here" appendix that Scott uses in the Cisco series. There are blank pages you can use to add your own notes and make this your journal, not mine.

Command Syntax Conventions

The conventions used to present command syntax in this book are as follows:

- **Boldface** indicates syntax that is entered literally as shown.
- *Italic* indicates syntax for which you supply actual values.
- Vertical bars | separate alternative, mutually exclusive choices.
- Square brackets [] indicate an optional element.
- Braces { } indicate a required choice.

CHAPTER 12

Using ntdsutil

This chapter provides information and commands concerning the following topics:

- Resetting the directory services restore mode password
- Changing the garbage collection logging level
- Moving Active Directory to a different drive
- Defragmenting Active Directory
- Performing an authoritative restore
- Removing a domain controller from Active Directory
- Seizing an operations master role

NOTE Commands in this chapter are run on a domain controller (DC) named DC1 in the pearson.pub domain.

TIP You should be familiar with **ntdsutil** commands and capabilities when preparing for the 70-640, 70-646, and 70-647 exams.

Resetting the Directory Services Restore Mode Password

The following steps show how to reset the Directory Services Restore Mode (DSRM) password.

Step	Command
1.	Start a command prompt with administrative permissions on a domain controller.
2.	Type ntdsutil and press Enter .
3.	Type set dsrm password and press Enter . This accesses the Reset DSRM Administrator Password prompt.
4.	Type reset password on server <i>servername</i> and press Enter . Substitute <i>servername</i> with the name of the domain controller.
5.	Type a new password and press Enter . Type the same password and press Enter again.
6.	Type quit and press Enter . Type quit and press Enter again.

Changing the Garbage Collection Logging Level

Garbage collection runs regularly in a DC and removes deleted (or tombstoned) objects from the database.

NOTE This is also known as online defragmentation.

When objects are deleted, it frees up space in the database but the database file size does not change. In other words, if the database is 100 MB, and then you delete 100 objects, the database size will still be 100 MB but it will have more free space. However, if you do an offline defragmentation, you can reclaim the free space. Before you do this, figure out how much free space you'll gain by doing the offline defragmentation.

If you change the garbage collection logging level, the garbage collection process will log Event ID 1646 (as shown in Figure 12-1) in the Directory Service log. This log entry shows how much free space an offline defragmentation will reclaim (only 2 MB in Figure 12-1).

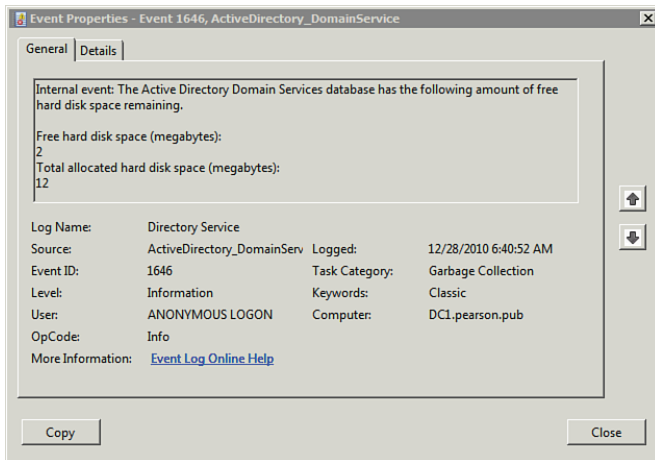


Figure 12-1 Event ID 1646 after changing the garbage collection logging level

TIP Before modifying the registry, you should create a backup.

The following steps show how to reset the garbage collection logging level.

Step	Command
1.	Click Start , type regedit , and press Enter to launch the Registry Editor .
2.	Browse to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics entry.
3.	Locate the Garbage Collection value and double-click it. Enter 1 as the value. Your display should look similar to Figure 12-2.
4.	Click OK . Close the Registry Editor .

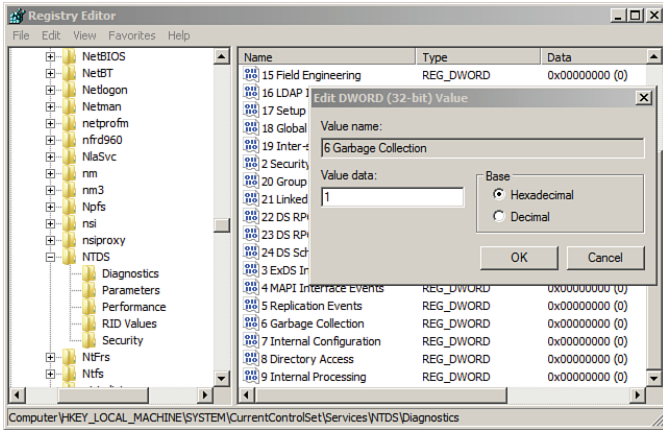


Figure 12-2 Changing the garbage collection logging level

Moving Active Directory to a Different Drive

You can sometimes improve the performance of Active Directory (AD) by moving the database file (`ntds.dit`) to a different physical drive. This can also be useful if you are running out of hard drive space. You can use the following steps to move the `ntds.dit` database file to a different location.

Step	Command
1.	<p>Launch a command prompt. Back up system state data with the following command. This command uses the D: drive as the backup target, but you can choose a different target based on your system. wbadmin start systemstate-backup -backuptarget:d: -quiet</p> <p>NOTE The Windows Server Backup feature must be installed for this step to work.</p> <p>TIP Although this step is not required, it ensures that you can recover your DC if something goes wrong. It takes some time to complete.</p>
2.	At the command, type net stop ntds and press Enter . When prompted to stop additional services, press Y to confirm. This stops AD and related services.
3.	Type ntdsutil and press Enter .
4.	Type activate instance ntds and press Enter .
5.	Type files and press Enter .
6.	<p>Type move db to e:\ntds and press Enter.</p> <p>NOTE You need to substitute the drive letter e: with a valid writable drive on your system. The folder doesn't need to exist because the move command creates it.</p>
7.	Type quit , and then press Enter twice to return to the command prompt.
8.	Type net start ntds and press Enter to restart AD. After it starts, you can launch ADUC to verify that everything still works.

Defragmenting Active Directory

AD performs an online defragmentation every 12 hours by default. This is normally all that's required. However, the online defragmentation does not reduce the size of the `ntds.dit` database file. If you have significantly fewer objects in AD than you had previously, you can shrink the size of the `ntds.dit` file by performing an offline defragmentation.

TIP An offline defragmentation compacts the file, and you can compact the file only when AD is not running. You can stop the service with the `net stop ntds` command. It's not necessary to reboot into Directory Services Restore Mode.

You can use the following steps to compact the database.

Step	Command
1.	<p>Launch a command prompt. Back up system state data with the following command. This command uses the D: drive as the backup target, but you can choose a different target based on your system. wbadmin start systemstate-backup -backuptarget:d: -quiet</p> <p>NOTE The Windows Server Backup feature must be installed for this step to work.</p> <p>TIP Although this step is not required, it ensures that you can recover your DC if something goes wrong. It takes some time to complete.</p>
2.	At the command, type net stop ntds and press Enter . When prompted to stop additional services, press Y to confirm. This stops AD and related services.
3.	Type ntdsutil and press Enter .
4.	Type activate instance ntds and press Enter .
5.	Type files and press Enter .
6.	Type compact to C:\compact and press Enter . You can use any target folder desired (other than C:\compact). Your display should be similar to Figure 12-3.
7.	<p>Type quit and press Enter. Type quit and press Enter again. This returns you to the command prompt.</p> <p>Although the following steps aren't required, they help ensure that you can return to the original configuration if something goes wrong.</p> <p>a. Create a backup folder named <code>ntdsbu</code> in the root of C by typing md C:\ntdsbu and pressing Enter.</p> <p>b. Type copy C:\windows\ntds\ntds.dit C:\ntdsbu\ntds.dit and press Enter.</p> <p>NOTE If you moved the <code>ntds.dit</code> file, you need to substitute the <code>C:\windows\ntds</code> folder for the actual location.</p> <p>c. Type copy C:\windows\ntds*.log C:\ntdsbu and press Enter.</p> <p>NOTE These steps create backup files of the <code>ntds.dit</code> AD database and the AD logs. If the <code>ntds</code> service is unable to restart, you can simply copy these files back to their original location.</p>

Step	Command
8.	Type <code>copy C:\compact\ntds.dit C:\windows\ntds\ntds.dit</code> and press Enter . When prompted to confirm the overwriting, type Y for yes.
9.	Type <code>del C:\windows\ntds*.log</code> and press Enter .
10.	Type <code>net start ntds</code> , and press Enter . This restarts the ntds service. After it starts, you can launch ADUC to verify that everything still works.

```

Administrator: Command Prompt - ntdsutl
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: files
file maintenance: compact to c:\compact
*** Error: Destination "c:\compact\ntds.dit" already exists - please remove
file maintenance: compact to c:\compact
Initiating DEFRAGMENTATION mode...
Source Database: e:\ntds\ntds.dit
Target Database: c:\compact\ntds.dit

          Defragmentation Status (% complete)
          0    10    20    30    40    50    60    70    80    90   100
          |-----|-----|-----|-----|-----|-----|-----|-----|-----|
          .....

It is recommended that you immediately perform a full backup
of this database. If you restore a backup made before the
defragmentation, the database will be rolled back to the state
it was in at the time of that backup.

Compactio is successful. You need to:
copy "c:\compact\ntds.dit" "e:\ntds\ntds.dit"
and delete the old log files:
del C:\windows\NTDS\*.log

File maintenance:

```

Figure 12-3 Performing an offline defragmentation

Performing an Authoritative Restore

When you do a normal nonauthoritative restore in a domain with more than one DC, the restored DC will replicate with other DCs in the domain to update itself. The restored DC will quickly have all the changes that occurred since the last backup. However, there are times when you want to restore objects authoritatively. In other words, when the restored DC comes back up, you want objects restored on the DC to be replicated to other DCs. You want this DC to communicate to all the other DCs that its change is the authoritative change.

For example, if an administrator accidentally deletes a user object and you perform a nonauthoritative restore, the user object will be deleted again as soon as the DC replicates with other DCs. However, you can restore the user object authoritatively, and you can even restore entire OUs authoritatively.

You can use the commands in the following table to authoritatively restore AD objects from the authoritative restore prompt in `ntdsutil`.

Restore Command	Comments
Restore OU. <pre>restore subtree dn</pre> authoritative restore: <pre>restore subtree "ou=sales,dc=pearson,dc=pub"</pre>	You can use this to restore an OU (including child OUs). The example command restores the Sales OU.
Restore Object. <pre>restore object dn</pre> authoritative restore: <pre>restore object "cn=Sally, ou=sales,dc=pearson,dc=pub"</pre>	This enables you to restore an individual object. The example command restores the Sally user object in the sales OU.

The following table shows the overall steps to perform an authoritative restore.

Step	Command
1.	Reboot the DC and press F8 to access Advanced Boot Options .
2.	Select Directory Services Restore Mode . When prompted, log on with the user name of .Administrator and the DSRM password.
3.	Restore AD nonauthoritatively from a backup. You can use the command-line backup tool, wbadmin , or any other method your organization has available. Do not reboot after the restore is complete. NOTE Chapter 27, "Using wbadmin ," covers the use of wbadmin to perform backup and restores of system state data.
4.	Launch a command prompt, type ntdsutil , and then press Enter .
5.	Type activate instance ntds and press Enter .
6.	Type authoritative restore and press Enter .
7.	At this point, determine whether you're restoring an OU or an object. The previous table showed the syntax to restore either an OU or an object. Type the restore command and press Enter . For example, to restore a user object, use the following format: <pre>restore object dn</pre> <pre>restore object "cn=Sally,ou=sales,dc=pearson,dc=pub"</pre> Or, to restore an OU, use the following format: <pre>restore subtree dn</pre> <pre>restore subtree "ou=sales,dc=pearson,dc=pub"</pre> NOTE This increments the update sequence number (USN) so that all other DCs consider it the most recent change.
8.	Type quit and press Enter twice to exit ntdsutil .
9.	Restart the DC normally.

Removing a Domain Controller from Active Directory

If you run **dcpromo** on a DC to remove AD, the AD database will be updated to show that this server is no longer a DC. However, if a DC fails, you won't be able to run **dcpromo**.

If the DC has failed, AD still thinks it's an active DC. This causes a wide variety of errors that can be resolved if you remove the DC from AD, as shown in the following steps.

Step	Command
1.	Start a command prompt with administrative permissions.
2.	Type ntdsutil and press Enter .
3.	Type metadata cleanup and press Enter . This accesses the metadata cleanup prompt.
4.	Type connections and press Enter . This accesses the connections prompt.
5.	Connect to an active DC in the domain with the following command. Substitute the FQDN of an active DC in your domain. connect to server <i>dc-fqdn</i> connect to server dc1.pearson.pub
6.	Type quit and press Enter . This brings you back to the metadata cleanup prompt.
7.	Type select operation target and press Enter . This accesses the select operation target prompt.
8.	Select the site where the damaged DC is located with the following commands. Substitute the number of the site in the second command based on the output of the list sites command. Type list sites and press Enter . Type select site <i>number</i> and press Enter .
9.	Select the damaged DC with the following commands. Substitute the number of the server in the second command based on the output of the list servers in site command. Type list servers in site and press Enter . Type select server <i>number</i> and press Enter .
10.	Type quit and press Enter . This brings you back to the metadata cleanup prompt.
11.	Type remove selected server and press Enter . This removes the instance of the server from AD.
12.	Type quit and press Enter .

Seizing an Operations Master Role

If a DC hosting a critical operations master role (previously called flexible single master operations role, [FSMO]) fails, you might need to have another DC take over the role. The best choice is to transfer the role while both servers are operational. However, if the role holder fails, you can seize the role using a DC that is operational.

TIP Seizing a role is a drastic operation. You should seize roles only when absolutely necessary. If you are seizing the Schema Master, the Domain Naming Master, or the RID Master roles, it's recommended that you don't bring the original DC back online in the domain.

The following steps show how to seize a role.

Step	Command
1.	Start a command prompt with administrative permissions on a domain controller.
2.	Type ntdsutil and press Enter .
3.	Type roles and press Enter . This accesses the fsmo maintenance prompt.
4.	Type connection and press Enter . This accesses the server connections prompt.
5.	Identify the fully qualified domain name (FQDN) of the operational DC. Substitute your DC's name in the following command: connect to server dc1.pearson.pub
6.	Type quit and press Enter . This brings you back to the fsmo maintenance prompt.
7.	Identify the role you want to seize. These are identified in ntdsutil as Infrastructure Master, Naming Master, PDC, RID Master, and Schema Master. Use one of the following commands to seize the role: seize infrastructure master seize naming master seize pdc seize rid master seize schema master
8.	A confirmation dialog box appears similar to Figure 12-4. Review it and click Yes if you want to seize the role. NOTE ntdsutil first tries to do a logical transfer. If the other DC is up and operational, it is transferred normally. If it fails, it seizes the role.
9.	Type quit and press Enter twice to exit ntdsutil .

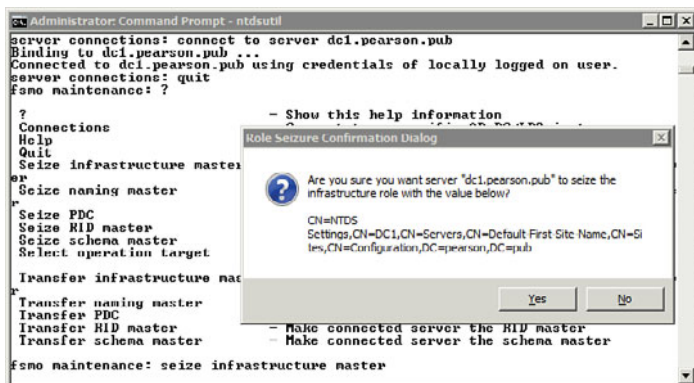


Figure 12-4 Seizing an operations role

This page intentionally left blank