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

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

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

Table of Contents

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 C|EH.

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** *servername* and press **Enter**. Substitute *servername* 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).

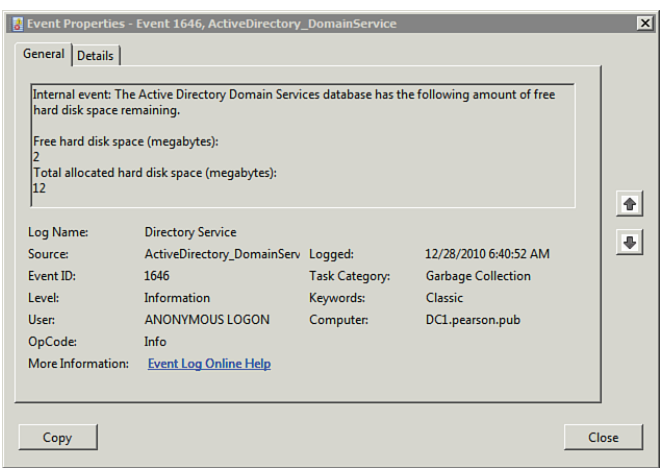

Figure 12-1 Event ID 1646 after changing the garbage collection logging level

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**.

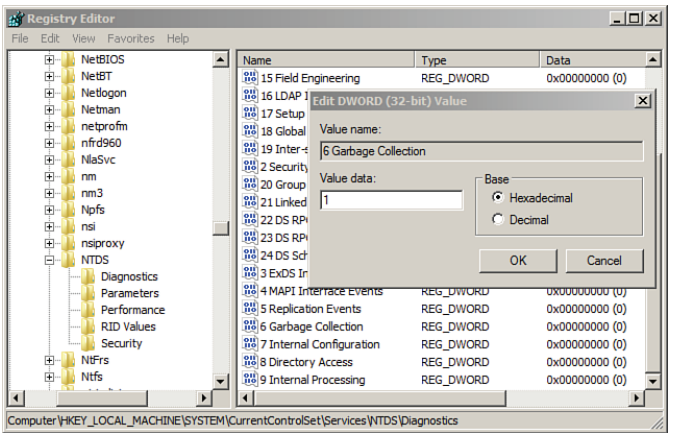

Figure 12-2 Changing the garbage collection logging level

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.	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** **NOTE** The Windows Server Backup feature must be installed for this step to work. **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.
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 **move db to e:\ntds** and press **Enter**. **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.
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.	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 systemstatebackup -backuptarget:d: -quiet** **NOTE** The Windows Server Backup feature must be installed for this step to work. **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.
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.	Type **quit** and press **Enter**. Type **quit** and press **Enter** again. This returns you to the command prompt. Although the following steps aren't required, they help ensure that you can return to the original configuration if something goes wrong. a. Create a backup folder named ntdsbu in the root of C by typing **md C:\ntdsbu** and pressing **Enter**. b. Type **copy C:\windows\ntds\ntds.dit C:\ntdsbu\ntds.dit** and press **Enter**. **NOTE** If you moved the ntds.dit file, you need to substitute the C:\windows\ntds folder for the actual location. c. Type **copy C:\windows\ntds*.log C:\ntdsbu** and press **Enter**. **NOTE** These steps create backup files of the ntds.dit AD database and the AD logs. If the ntds service is unable to restart, you can simply copy these files back to their original location.

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

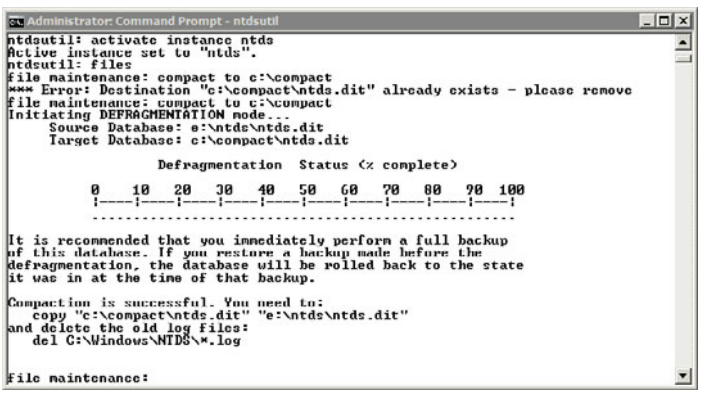

Figure 12-3 Performing an offline defragmentation

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. `restore subtree` *dn* authoritative restore: `restore subtree "ou=sales,dc=pearson,dc=pub"`	You can use this to restore an OU (including child OUs). The example command restores the Sales OU.
Restore Object. `restore object` *dn* authoritative restore: `restore object "cn=Sally, ou=sales,dc=pearson,dc=pub"`	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: **restore object** *dn* **restore object "cn=Sally,ou=sales,dc=pearson,dc=pub"** Or, to restore an OU, use the following format: **restore subtree** *dn* **restore subtree "ou=sales,dc=pearson,dc=pub"** **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** *dc-fqdn* **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** *number* 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** *number* 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**.

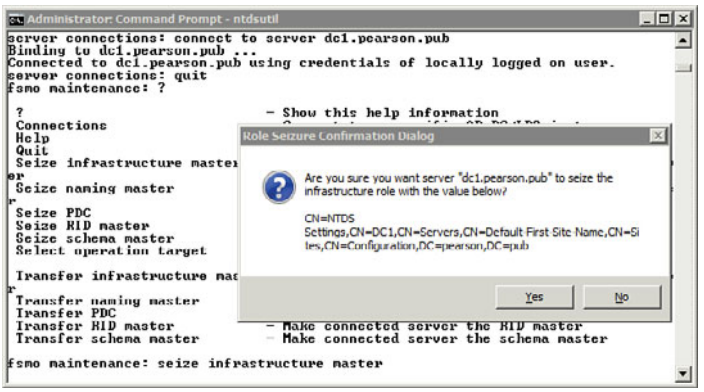

Figure 12-4 Seizing an operations role

This page intentionally left blank