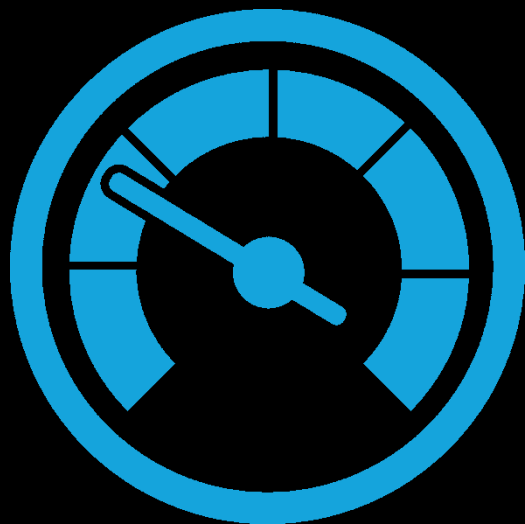


WINDOWS TROUBLESHOOTING SERIES



Troubleshooting Windows Server with PowerShell

Derek Schauland
Donald Jacobs

EXTRAS ONLINE

apress®

Troubleshooting Windows Server with PowerShell



Derek Schauland
Donald Jacobs

Apress®

Troubleshooting Windows Server with PowerShell

Derek Schauland
Greenville, Wisconsin, USA

Donald Jacobs
Appleton, Wisconsin, USA

ISBN-13 (pbk): 978-1-4842-1850-1
DOI 10.1007/978-1-4842-1851-8

ISBN-13 (electronic): 978-1-4842-1851-8

Copyright © 2016 by Derek Schauland and Donald Jacobs

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director: Welmoed Spahr

Lead Editor: Gwenan Spearing

Development Editor: Douglas Pundick

Technical Reviewer: Adam Driscoll

Editorial Board: Steve Anglin, Pramila Balen, Louise Corrigan, Jim DeWolf, Jonathan Gennick,

Robert Hutchinson, Celestin Suresh John, James Markham, Susan McDermott,

Matthew Moodie, Douglas Pundick, Ben Renow-Clarke, Gwenan Spearing

Coordinating Editor: Melissa Maldonado

Copy Editor: Kim Burton-Weisman

Compositor: SPi Global

Indexer: SPi Global

Artist: SPi Global

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springer.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a Delaware corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

Apress and friends of ED books may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Special Bulk Sales–eBook Licensing web page at www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this text is available to readers at www.apress.com. For detailed information about how to locate your book's source code, go to www.apress.com/source-code/.

Printed on acid-free paper

For Laura—thanks for the encouragement.

For Nyla—keep learning.

Contents at a Glance

About the Authors..... xiii

About the Technical Reviewer xv

Acknowledgments xvii

Introduction xix

■ Chapter 1: Getting Started 1

■ Chapter 2: Managing the Windows Event Log 17

**■ Chapter 3: Gathering and Reporting Detailed Information
from a Computer 35**

■ Chapter 4: Installed Applications 53

■ Chapter 5: Windows Update 65

■ Chapter 6: Manage Running Processes on a Target System 75

■ Chapter 7: Review and Manage Services with PowerShell 89

■ Chapter 8: Continuing to Learn As PowerShell Evolves..... 103

Index..... 117

Contents

About the Authors.....	xiii
About the Technical Reviewer	xv
Acknowledgments	xvii
Introduction	xix
■ Chapter 1: Getting Started	1
Getting to Know PowerShell.....	2
GUI Tools vs. PowerShell	3
The Basics of PowerShell.....	4
Working with Variables.....	4
CMD Is Dead—Long Live PowerShell.....	5
Why All the Drives?	5
The Natural Progression of Tool Building	6
PowerShell Is Not Going Away	7
What Does this Do for PowerShell?	8
Chapters in this Book	8
Assumptions Used in this Book.....	9
How to Let PowerShell Help You Learn More	11
Summary.....	15
More Reading	16

■ Chapter 2: Managing the Windows Event Log	17
What Can Windows Capture?	17
Accessing the Event Log Information.....	18
Get-EventLog	19
Get-WinEvent.....	22
Why Choose One cmdlet over Another?.....	22
Getting Logs from Remote Computers	23
Shaping the Gathered Information	24
Comma-Separated Values	24
Creating an HTML Report.....	27
What Else Can Be Done with this Information?.....	27
Formatting HTML for Readability.....	27
HTML Formatting with a Function	28
Can PowerShell Use the Event Log to Store Information?.....	32
Summary	33
■ Chapter 3: Gathering and Reporting Detailed Information from a Computer	35
Gathering Disk Space	35
Disks First.....	36
Logical Disks	37
Listing Shares.....	38
NTFS Permissions	41
Getting the ACLs	42
Setting the ACLs	43
Hardware.....	45
Computer System Information	48

Processor Information	49
Troubleshooting	51
The Difference Between WMI and CIM	51
Remote Queries	51
Next Steps	52
Summary	52
■ Chapter 4: Installed Applications	53
Obtaining a List of Installed Applications	53
Using the CIM Object	54
Using the Registry Keys	58
Arrays	60
Next Steps	62
Summary	63
■ Chapter 5: Windows Update	65
Get-HotFix	66
Scenario	66
Resolution	66
Using WMI or CIM	67
Details of Get-HotFix Results	67
Checking When a Computer Was Rebooted	68
Uninstalling a Hot Fix	71
Improvements to this Function	71
Pending Restarts	72
Summary	74

■ Chapter 6: Manage Running Processes on a Target System	75
Working with Processes	75
Filtering by Process ID or Name	78
Sorting and Selecting Information Needed	79
Working with Returned Data	81
Delivering the Goods: A Quick Sidestep to Sending Email	82
Collecting Information from a Remote Computer or Computers	82
Other Ways to Improve the Script	83
Starting and Stopping Processes	84
When Start-Process and Stop-Process Are Useful	85
Select First, Then Again, and Then Stop	86
Using WMI or CIM to Work with Processes	86
Using the CIM cmdlets	87
Summary	88
■ Chapter 7: Review and Manage Services with PowerShell	89
Access to Services with PowerShell	89
Gathering Service Information	90
Actions on Services	90
Enter WMI	95
Summary	101
■ Chapter 8: Continuing to Learn As PowerShell Evolves.....	103
Building Modules.....	103
Desired State Configuration	105
What Is Desired State Configuration (DSC)?.....	106
Auditing Only	106
Applying Configurations: Make It So	106
What Does a DSC Configuration Look Like?	107

What Are Some Practical Applications of DSC?	107
Starting or Stopping Services	107
Installing Necessary Roles or Features	108
Fixing Configuration Drift: Wrongly Installed Applications.....	108
Ensuring That Files or Folders Exist	108
Working with DSC to Ensure IIS Is Installed	108
PowerShell Remoting	109
How Do I Enable Remoting?	110
A Remote PowerShell Session	110
Using Scheduled Jobs in PowerShell	111
Scheduled Jobs Options	111
Scheduled Job Triggers	112
Creating the Scheduled Job	113
Job Verification.....	113
Getting Scheduled Job Results	114
More Learning and Additional Resources.....	115
Summary	115
Index.....	117

About the Authors



Derek Schauland is a Microsoft MVP with 18 years' experience configuring everything from Windows NT 4.0 environments to Windows Server 2016. He has worked in help desk and systems administrator roles helping companies and end users alike handle the challenges that can accompany the Windows experience. He has written for publications ranging from white papers for internal publication, to *Redmond Magazine* and *TechRepublic*, and books for Microsoft Press. When he isn't helping configure development or cloud environments, writing for the next great publication, or working to put on local technology events, he can be found tasting the latest craft beer, watching movies, or spending time with family and friends.



Donald Jacobs began his IT career back when Windows NT was the biggest and best new technology in the field. Since that time, he has earned a multitude of Microsoft certifications, including MCSE Server Infrastructure 2012, MCSA Office 365, MCITP Enterprise Administrator 2008, and MCTS for Windows 7. He has taught Microsoft's Certified PowerShell and Windows Server courses as a Microsoft Certified Trainer. Currently, Donald supports clients and customers with Microsoft products, particularly PowerShell, Azure, Office 365, Active Directory, Exchange, and Windows Server. In his downtime, he enjoys spending time with his family, watching hockey, and playing Dungeons & Dragons.