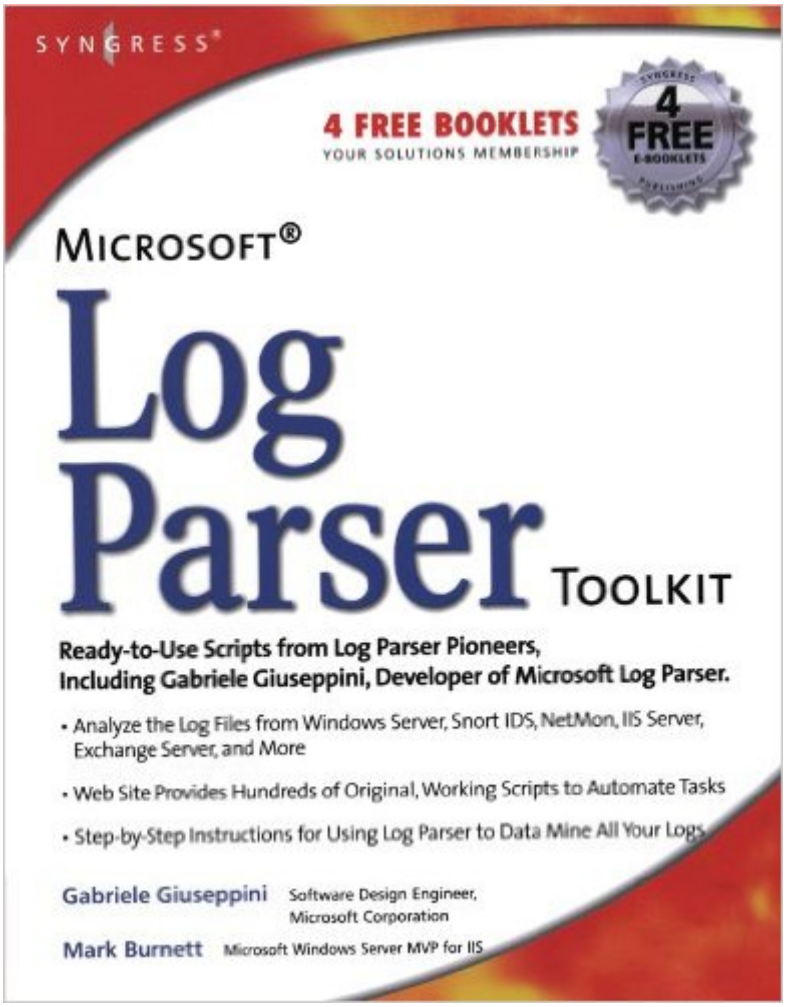
Microsoft Log Parser Toolkit: A Complete Toolkit For Microsoft's Undocumented Log Analysis Tool



Synopsis

Written by Microsoft's Log Parser developer, this is the first book available on Microsoft's popular yet undocumented log parser tool. The book and accompanying Web site contain hundreds of customized, working scripts and templates that system administrators will find invaluable for analyzing the log files from Windows Server, Snort IDS, ISA Server, IIS Server, Exchange Server, and other products. System administrators running Windows, Unix, and Linux networks manage anywhere from 1 to thousands of operating systems (Windows, Unix, etc.), Applications (Exchange, Snort, IIS, etc.), and hardware devices (firewalls, routers, etc.) that generate incredibly long and detailed log files of all activity on the particular application or device. This book will teach administrators how to use Microsoft's Log Parser to data mine all of the information available within these countless logs. The book teaches readers how all queries within Log Parser work (for example: a Log Parser query to an Exchange log may provide information on the origin of spam, viruses, etc.). Also, Log Parser is completely scriptable and customizable so the book and accompanying Web site will provide the reader with hundreds of original, working scripts that will automate these tasks and provide formatted charts and reports detailing the results of the queries.Written by Microsoft's sole developer of Log Parser, this is the first book available on the powerful yet completely undocumented product that ships with Microsoft's IIS, Windows Advanced Server 2003, and is available as a free download from the Microsoft Web siteThe book and accompanying Web site contain dozens of original, working Log Parser scripts and templates for Windows Server, ISA Server, Snort IDS, Exchange Server, IIS, and more!This book and accompanying scripts will save system administrators countless hours by scripting and automating the most common to the most complex log analysis tasks

Book Information

Paperback: 350 pages
Publisher: Syngress; 1 edition (February 24, 2005)
Language: English
ISBN-10: 9781932266528
ISBN-13: 978-1932266528
ASIN: 1932266526
Product Dimensions: 7.1 x 1.1 x 9.2 inches
Shipping Weight: 2 pounds (View shipping rates and policies)
Average Customer Review: 4.4 out of 5 starsÂ Â See all reviewsÂ (17 customer reviews)

Best Sellers Rank: #858,337 in Books (See Top 100 in Books) #77 inÂ Books > Computers & Technology > Software > Utilities #130 inÂ Books > Computers & Technology > Programming > Microsoft Programming > SQL Server #285 inÂ Books > Computers & Technology > Business Technology > Windows Server

Customer Reviews

This review is not so much about the book’s content as it is the quality of this particular book’s Kindle version. I’ll be purchasing the physical book and will review its content once I have a chance to get into it.I’ve read a ton of Kindle books, and have bought a number of Kindle versions of tech books, and never have I had this issue. I was so excited to get this book because I need to collect web traffic information for literally thousands of IIS servers. What a disappointment. The regular text of of the book is completely normal--you can resize it, change the color, etc. However, the log parser examples are apparently images, and many are absolutely, hilariously, MICROSCOPIC in the KIndle version. They don’t enlarge when the text is enlarged and they don’t copy. I tried a number of work arounds to enlarge them (mainly doing a screen capture and copying them into Word or a graphics program), and since they’re so small they don’t enlarge well--they just look like a bunch of pixels. I tried reading the book on a Kindle, my Samsung S5, and in Kindle for PC, and it’s all the same. On my phone, which has a nice big screen, it’s really hard to tell that the examples are actually text--they just look like fuzzy lines.So, now I have to pay more for the physical book and lug it around with me rather than having the convenience and flexibility of a Kindle version. That really sucks, as I’m a huge fan of KIndle books (not to mention a fan of paying less).

This is a complete reference for utilizing the Microsoft’Log Parser Tool in real world scenarios.The authors do an outstanding job of bringing you from the basics of Log Parser through advanced techniques and tricks. I have thoroughly enjoyed reading it end to end, and have begun utilizing Log Parser in my daily log assessment routines. The Tips, Swiss Army Knifes, and Master Craftsman sidebars prove extremely creative and helpful.

Log Parser is a Swiss-army knife tool that provides users with a powerful set of basic features that analyze, slice, and report on a large variety of information.The idea of writing this book stemmed from the realization that most of the Log Parser users find it difficult to harness the power of the tool and discover how to customize and use its basic features to complete the task at hand."The Microsoft Log Parser Toolkit" has been written by users that have been employing the tool for years

to manage their IT systems, and shows the scripts, queries, and tricks that they use on their jobs.The first chapter gives you a thorough understanding of the Log Parser SQL-like language (how do I filter Event Log entries? How do I search for specific Web requests in time? How do I calculate statistics?), introduces you to the many input and output formats supported by version 2.2 (including the newest ADS, TSV, and NETMON input formats and the CHART and SYSLOG output formats), and delves into those little-known additional features that enhance this tool's productivity (including incremental parsing and output multiplexing).The next 10 chapters provide solutions and working examples for all the problems that can be quickly solved with Log Parser.With these chapters you will learn how to script the tool features, how to write input format plug-ins to provide your own data to Log Parser, and how to best employ its input and output formats to create charts, reports, and web applications.You will see techniques used by the authors to perform security auditing and intrusion detection, to analyze server performance, and to manage and monitor IIS servers.Regardless of whether you are new to Log Parser, or if you are an experienced user, this book will give you new ideas and discover a few new tricks that you never thought of before!

This tool is amazing in that it supports a variety input and output formats including reading in syslog and outputting into databases are pretty Excel charts. The filtering uses an SQL syntax. The tool comes with a DLL that can be registered, so that scripters (VBScript, Perl, JScript, etc.) can access the power of this tool.This book not only covers the tool (alternative being to scrape the network for complex incomprehensible snippets), but shows real world practical solutions with the tool, from analyzing web logs, system events, security and network scans, etc.This tool is just heavensend for analysis and transforming of any data in a variety of formats. The book and tool go hand-in-hand, and I highly recommend incorporating this into your tool (and book) into your tool kit and/or scripting endeavors immediately.

Log Parser by it self is a wonderful tool, this book lets you get up and running with it in no time.Additionally it gives a great insight on logs. This book is essential for any admin that wants to keep with "the going on" on his network without running agents everywhere. Log Parser toolkit lets you make logs readable (what a novel concept) without the need for heavy programming, all the scripts are included and really easy to customize. If you keep any type of log this will make your life easier and can save you major head hakes. My only recommendation is when you get one for your self, don't forget to get one for your IIS admin and your security guy, or be ready to share it. Enjoy it...

Microsoft Log Parser Toolkit: A Complete Toolkit for Microsoft's Undocumented Log Analysis Tool The Garden Journal, Planner and Log Book: Repeat successes & learn from mistakes with complete personal garden records. 28 adaptable year-round forms, ... (The Garden Journal Log Books) (Volume 1) Microsoft Surface Pro 4 & Microsoft Surface Book: The Beginner's Guide to Microsoft Edge, Cortana & Mail App on Microsoft Surface Pro 4 & Microsoft Surface Book Diabetes Journal Log Book: Portable 6in x 9in Diabetes, Blood Sugar Log. Daily Readings For 53 weeks. Before & After for Breakfast, Lunch , Dinner, Snacks. Bedtime. With Daily Notes (Fitness) Dive Log: A Divemaster's Dive Log Windows Forensic Analysis Toolkit, Third Edition: Advanced Analysis Techniques for Windows 7 Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 7 Undocumented: How Immigration Became Illegal Living the Dream: New Immigration Policies and the Lives of Undocumented Latino Youth (New Critical Viewpoints on Society) The DREAMers: How the Undocumented Youth Movement Transformed the Immigrant Rights Debate Lives in Limbo: Undocumented and Coming of Age in America Identity, Social Activism, and the Pursuit of Higher Education: The Journey Stories of Undocumented and Unafraid Community Activists (Critical Studies of Latinos/as in the Americas) Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit The Complete Runner's Day-by-Day Log 2017 Calendar Bundle: New Perspectives on Microsoft Project 2010: Introductory + Microsoft Project 2010 60 Day Trial CD-ROM for Shelly/Rosenblatt's Systems Analysis and Design Microsoft Excel 2013 Data Analysis and Business Modeling: Data Analysis and Business Modeling (Introducing) XDA Developers' Android Hacker's Toolkit: The Complete Guide to Rooting, ROMs and Theming Enhanced Microsoft Excel 2013: Illustrated Complete (Microsoft Office 2013 Enhanced Editions) The Pokemon Go Addiction: Learning to Log Off And Avoid A Troubling Obsession Construction Daily Project Log for Construction & Maintenance