1.

Record Nr.	UNINA9910783282403321
Autore	Giuseppini Gabriele
Titolo	Microsoft log parser toolkit [[electronic resource] /] / Gabriele Giuseppini
Pubbl/distr/stampa	Rockland, MA, : Syngress Publishing, c2004
ISBN	1-281-03583-1 9786611035839 0-08-048939-7 1-59749-028-8
Edizione	[1st edition]
Descrizione fisica	1 online resource (465 p.)
Disciplina	005.74/068 511.3
Soggetti	Parsing (Computer grammar) Computational linguistics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di contenuto	Cover; Contents; Foreword; Chapter 1 Introducing Log Parser; Chapter 2 Monitoring IIS; Chapter 3 Exploring the Windows Event Log; Chapter 4 Examining Network Traffic and Performance Logs with Log Parser; Chapter 5 Managing Snort Alerts; Chapter 6 Managing Log Files; Chapter 7 Investigating Intrusions; Chapter 8 Security Auditing; Chapter 9 Enhancing Log Parser; Chapter 10 Formatting, Reporting, and Charting; Chapter 11 Handling Complex Data; Appendix A SQL Grammar Reference; Appendix B Function Reference; Appendix C Input Format Reference; Output Format Reference; Index; Related Titles
Sommario/riassunto	HIGHLIGHTWritten 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,