1. Record Nr. UNINA9910464160003321

Autore	Miller James
Titolo	Mastering Splunk : optimize your machine-generated data effectively by developing advanced analytics with Splunk / / James Miller
Pubbl/distr/stampa	Birmingham, England : , : Packt Publishing, , 2014 ©2014
ISBN	1-78217-384-6
Edizione	[1st edition]
Descrizione fisica	1 online resource (344 p.)
Collana	Professional Expertise Distilled
Disciplina	006.754
Soggetti	Data mining - Computer programs Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover; Copyright; Credits; About the Author; About the Reviewers; www.PacktPub.com; Table of Contents; Preface; Chapter 1: The Application of Splunk; The definition of Splunk; Keeping it simple; Universal file handling; Confidentiality and security; The evolution of Splunk; The Splunk approach; Conventional use cases; Investigational searching; Searching with pivot; The event timeline; Monitoring; Alerting; Reporting; Visibility in the operational world; Operational intelligence; A technology-agnostic approach; Decision support - analysis in real time; ETL analytics and preconceptions The complements of SplunkODBC; Splunk - outside the box; Customer Relationship Management; Emerging technologies; Knowledge discovery and data mining; Disaster recovery; Virus protection; The enhancement of structured data; Project management; Firewall applications; Enterprise wireless solutions; Hadoop technologies; Media measurement; Social media; Geographical Information Systems; Mobile Device Management; Splunk in action; Summary; Chapter 2: Advanced Searching; Searching in Splunk; The search dashboard; The new search dashboard; The Splunk search mechanism The Splunk quick reference guide Please assist me, let me go; Basic optimization; Fast, verbose, or smart?; The breakdown of commands; Understanding the difference between sparse and dense; Searching for operators, command formats, and tags; The process flow; Boolean

expressions; You can quote me, I'm escaping; Tag me Splunk!; Assigning a search tag; Tagging field-value pairs; Wild tags!; Disabling and deleting tags; Transactional searching; Knowledge management; Some working examples; Subsearching; Output settings for subsearches; Search Job Inspector; Searching with parameters
The eval statement A simple example; Splunk macros; Creating your own macro; Using your macros; The limitations of Splunk; Search results; Some basic Splunk search examples; Additional formatting; Summary; Chapter 3: Mastering Tables, Charts, and Fields; Tables, charts, and fields; Splunking into tables; The table command; The Splunk rename command; Limits; Fields; An example of the fields command; Returning search results as charts; The chart command; The split-by fields; The where clause; More visualization examples; Some additional functions; Splunk bucketing
Reporting using the time chart command Arguments required by the time chart command; Bucket time spans versus per_* functions; Drilldowns; The drilldown options; The basic drilldown functionality; Row drilldowns; Cell drilldowns; Chart drilldowns; Legends; Pivot; The pivot editor; Working with pivot elements; Filtering your pivots; Split; Column values; Pivot table formatting; A quick example; Sparklines; Summary; Chapter 4: Lookups; Introduction; Configuring a simple field lookup; Defining lookups in Splunk Web; Automatic lookups; The Add new page; Configuration files
Implementing a lookup using configuration files - an example

Sommario/riassunto

This book is for those Splunk developers who want to learn advanced strategies to deal with big data from an enterprise architectural perspective. You need to have good working knowledge of Splunk.