1.

Record Nr.	UNINA9910452485803321
Autore	Bumgarner Vincent
Titolo	Implementing Splunk [[electronic resource]] : big data reporting and development for operational intelligence : learn to transform your machine data into valuable IT and business insights with this comprehensive and practical tutorial / / Vincent Bumgarner
Pubbl/distr/stampa	Birmingham, : Packt Pub., 2013
ISBN	1-84969-329-3 1-299-19842-2
Edizione	[1st edition]
Descrizione fisica	1 online resource (448 p.)
Collana	Community experience distilled
Disciplina	006.78
Soggetti	Electronic data processing Database management 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 Splunk Interface; Logging in to Splunk; The Home app; The top bar; Search app; Data generator; The Summary view; Search; Actions; Timeline; The field picker; Fields; Search results; Options; Events viewer; Using the time picker; Using the field picker; Using Manager; Summary; Chapter 2: Understanding Search; Using search terms effectively; Boolean and grouping operators; Clicking to modify your search; Event segmentation; Field widgets; Time; Using fields to search Using the field pickerUsing wildcards efficiently; Only trailing wildcards are efficient; Wildcards are tested last; Supplementing wildcards in fields; All about time; How Splunk parses time; How Splunk stores time; How Splunk displays time; How time zones are determined and why it matters; Different ways to search against time; Specifying time in-line in your search; _indextime versus _time; Making searches faster; Sharing results with others; Saving searches for reuse; Creating alerts from searches; Schedule; Actions; Summary; Chapter 3: Tables, Charts, and Fields; About the pipe symbol

Using top to show common field valuesControlling the output of top; Using stats to aggregate values; Using chart to turn data; Using timechart to show values over time; timechart options; Working with fields; A regular expression primer; Commands that create fields; eval; rex; Extracting loglevel; Using the Extract Fields interface; Using rex to prototype a field; Using the admin interface to build a field; Indexed fields versus extracted fields; Summary; Chapter 4: Simple XML Dashboards; Why build a dashboard?; Using wizards to build dashboards; Scheduling the generation of dashboards

When to edit the XML directly?UI Examples app; Building Forms; Creating a form from a dashboard; Driving multiple panels from one form; Post-processing search results; Post-processing limitations; Panel 1; Panel 2; Panel 3; Final XML; Summary; Chapter 5: Advanced Search Examples; Using subsearches to find loosely related events; Subsearch; Subsearch caveats; Nested subsearches; Using transaction; Using transaction to determine the session length; Calculating the aggregate of transaction statistics; Combining subsearches with transaction; Determining concurrency

Using transaction with concurrencyUsing concurrency to estimate server load; Calculating concurrency with a by clause; Calculating events per slice of time; Using timechart; Calculating average requests per minute; Calculating average events per minute, per hour; Rebuilding top; Summary; Chapter 6: Extending Search; Using tags to simplify search; Using event types to categorize results; Using lookups to enrich data; Defining a lookup table file; Defining a lookup definition; Defining an automatic lookup; Troubleshooting lookups; Using macros to reuse logic; Creating a simple macro

Creating a macro with arguments

Sommario/riassunto	Learn to effectively use, configure, deploy and extend Splunk and implement its powerful capabilities