

2012-01-16 12:55 - TechWorld:

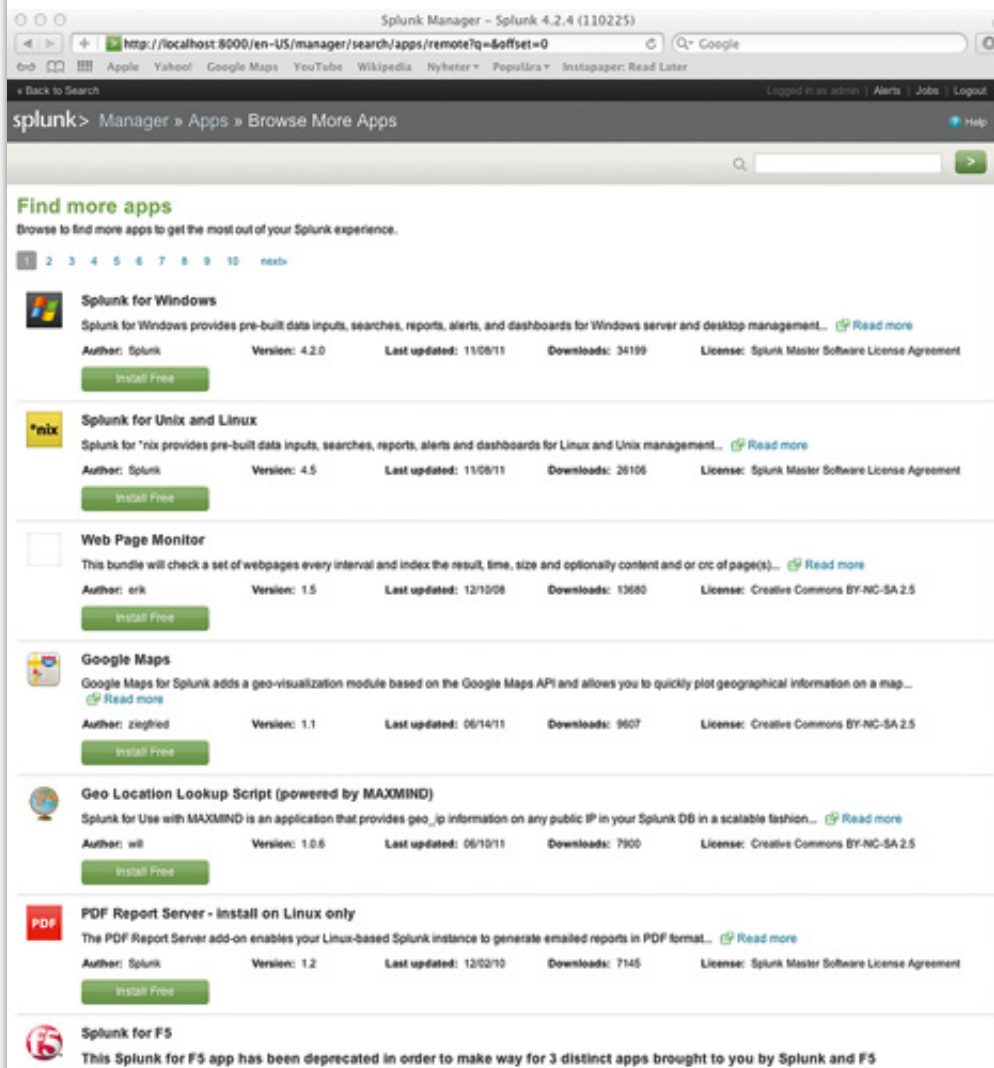
# Find the right answers in no time with Splunk

By Robert Ilijason

**TEST Solving problems is easy when the bias is well identified. With Splunk you to understand the basic problem in no time. But the case that you are willing to spend time on configuration.**

**Do you work with to resolve critical situations within the IT infrastructure?** If so, do you know how important it is to quickly find the problem source. That is what the developers of Splunk say they can help you with.

**In practice, it is a smart indexing tool.** You upload all logs and files you want searchable, and after all on-site analysis of Splunk content current.



The screenshot shows the Splunk Manager interface for version 4.2.4 (110225). The browser address bar shows the URL <http://localhost:8000/en-US/manager/search/apps/remote?q=&offset=0>. The page title is "splunk> Manager > Apps > Browse More Apps". The main content area is titled "Find more apps" and contains a list of available apps. Each app entry includes a description, author, version, last updated date, download count, and license. An "Install Free" button is provided for each app.

App Name	Author	Version	Last updated	Downloads	License
Splunk for Windows	Splunk	4.2.0	11/08/11	34199	Splunk Master Software License Agreement
Splunk for Unix and Linux	Splunk	4.5	11/08/11	26106	Splunk Master Software License Agreement
Web Page Monitor	erik	1.5	12/10/08	13680	Creative Commons BY-NC-SA 2.5
Google Maps	Ziegfried	1.1	06/14/11	9607	Creative Commons BY-NC-SA 2.5
Geo Location Lookup Script (powered by MAXMIND)	will	1.0.6	06/10/11	7900	Creative Commons BY-NC-SA 2.5
PDF Report Server - install on Linux only	Splunk	1.2	12/02/10	7145	Splunk Master Software License Agreement
Splunk for FS					

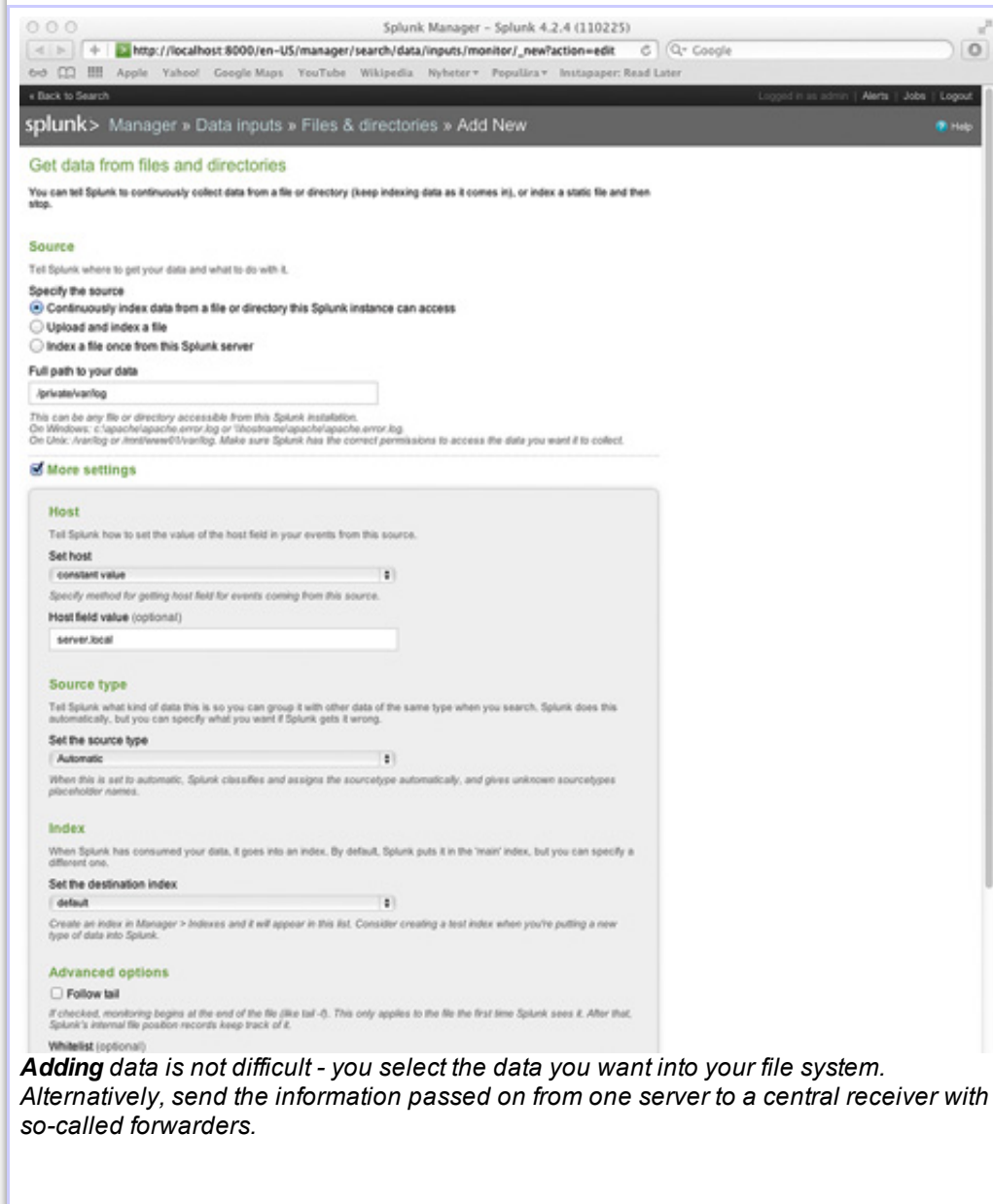
**There are many additions to download the Splunk, but unfortunately missing packages for many common systems. Thus expect to have put a lot of time on configuration for everything to be really good.**

## Search in all layers

You can search through all the layers and see what happened at a certain time. If you find a term that seems strange, you can click on it and immediately see if it also appeared in other places.

If you are unsure of the syntax will show you a help window how to continue. The searches are lightning fast and move the timeline requires only one keystroke.

**Recurring issues can be saved.** Do you want a graphical representation it is possible to create reports, and you can nail down important items on the so-called instrumentpaneler. Reaktiv analysis is what the tool is primarily created for, but it is possible to build creative solutions, not least that you can feed information from custom built scripts.



### Even in real time

Since Splunk examine logs regularly you can also use the tool for real-time analysis. For example you can instantly see if customers suddenly leave your site faster than usual, or if a server suddenly work a lot harder than usual. Do not want to keep your eyes on the screen all the time, you can create alarms that keeps track for you.

**Besides all this** there are additional modules for download from Splunks online store that is built into the tool. Almost everything is free, which is good, but unfortunately it is a bit thin on features. What is really missing is a ready-made packages for all major products, such as Oracle DB, IBM Infosphere, and Apple OS X. To configure Splunk takes up a lot of time if there is a lot of monitoring.

### TechWorld conclusion

**In conclusion, we must admit** that this is one of the best tools for IT administrators on the market right now. Splunk helps you to really quickly identify the root cause of a problem, and it is in many cases, the hard part - to solve the problem is usually easier.

It is almost every IT technicians duty to download friversionen of Splunk and self test how the tool can help.

## FACTS

# Splunk

**Product:** Splunk version 4.2.4

**Manufacturer:** Splunk

**Contact:** www.splunk.com

**Indicative price:** Free up to 500 MB per day

**Platform support:** Windows, Linux, Solaris, OS X, FreeBSD, AIX, HP-UX

Simple and very powerful.

Allows you quickly click their way through large volumes of data and find valuable information.

The screenshot shows the Splunk Search interface. At the top, the search bar contains the query `source=private/var/log/kernel.log`. Below the search bar, a bar chart shows the distribution of 14,403 matching events over time. The timeline view shows events from Saturday, October 8, 2011, to Saturday, November 12, 2011. The interface also displays a list of log events with details such as timestamp, host, source type, and source.

Event ID	Timestamp	Host	Source Type	Source	Message
1	Nov 17 20:04:26	host:server	syslog	private/var/log/kernel.log	server kernel[0]: nstat_lookup_entry failed: 2
2	Nov 17 20:04:24	host:server	syslog	private/var/log/kernel.log	server kernel[0]: IOsurface: buffer allocation size is zero
3	Nov 17 20:04:24	host:server.local	syslog	private/var/log/kernel.log	--- last message repeated 9 times ---
4	Nov 17 20:04:00	host:server	syslog	private/var/log/kernel.log	server kernel[0]: nstat_lookup_entry failed: 2
5	Nov 17 20:03:58	host:server	syslog	private/var/log/kernel.log	server kernel[0]: IOsurface: buffer allocation size is zero
6	Nov 17 20:03:55	host:server	syslog	private/var/log/kernel.log	server kernel[0]: nstat_lookup_entry failed: 2
7	Nov 17 20:03:45	host:server	syslog	private/var/log/kernel.log	server kernel[0]: IOsurface: buffer allocation size is zero
8	Nov 17 20:03:04	host:server	syslog	private/var/log/kernel.log	server kernel[0]: nstat_lookup_entry failed: 2
9	Nov 17 20:00:03	host:server	syslog	private/var/log/kernel.log	server kernel[0]: nstat_lookup_entry failed: 2
10	Nov 17 19:59:33	host:server	syslog	private/var/log/kernel.log	server kernel[0]: IOsurface: buffer allocation size is zero



Unfortunately requires a lot of configuration.

### GRADE

Functions and features: 24 of 30

Installation: 7 out of 10

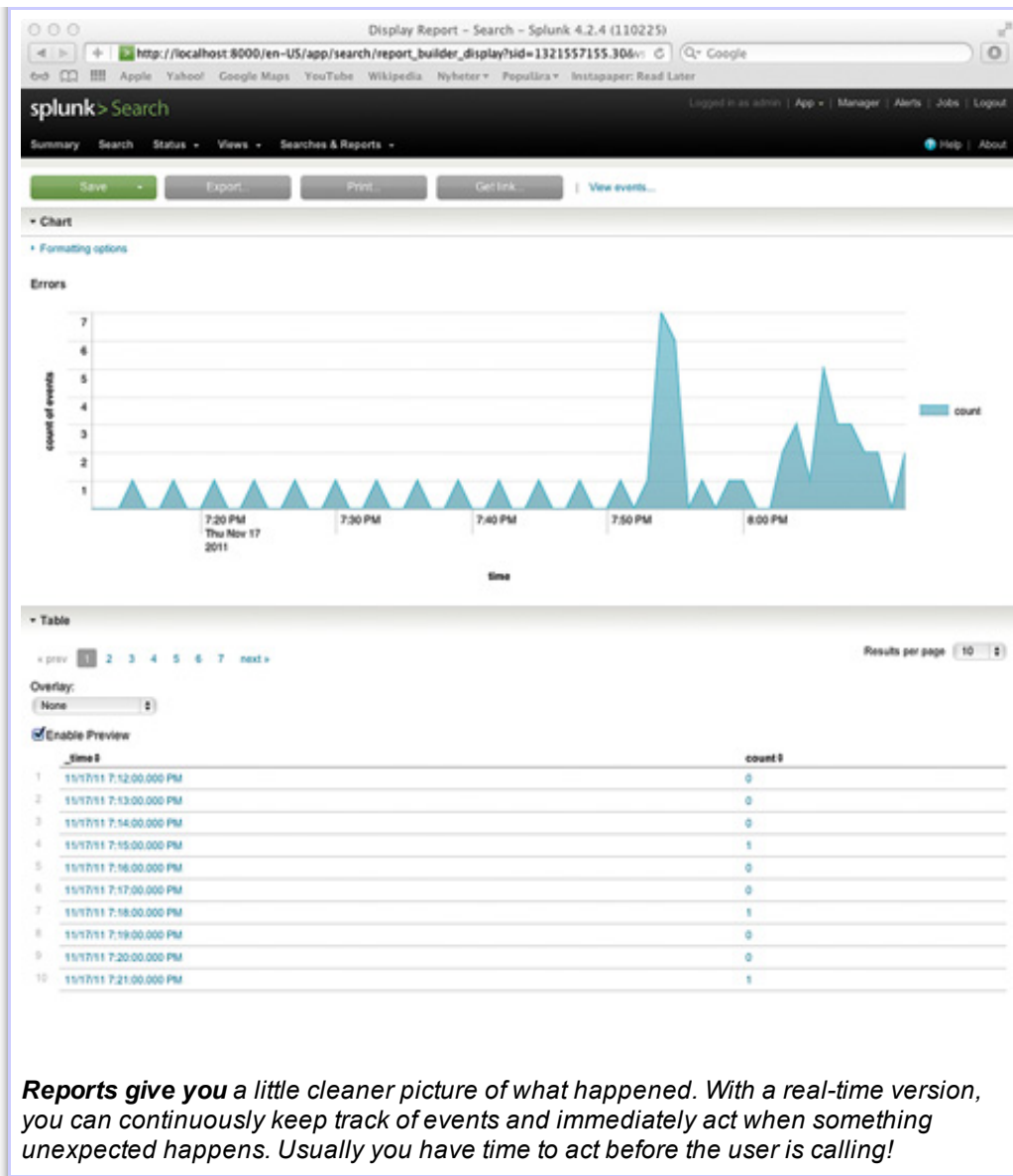
Ease of use: 26 of 30

Platform Support: 9 of 10

Speed: 18 of 20

TOTAL: 84 of 100

*Do you want to look at what has happened in a log file, just click on it. Splunk will show you both the timeline and details. From here you can drill your way down in the time dimension or test new search terms.*



**Reports give you** a little cleaner picture of what happened. With a real-time version, you can continuously keep track of events and immediately act when something unexpected happens. Usually you have time to act before the user is calling!