splunk>

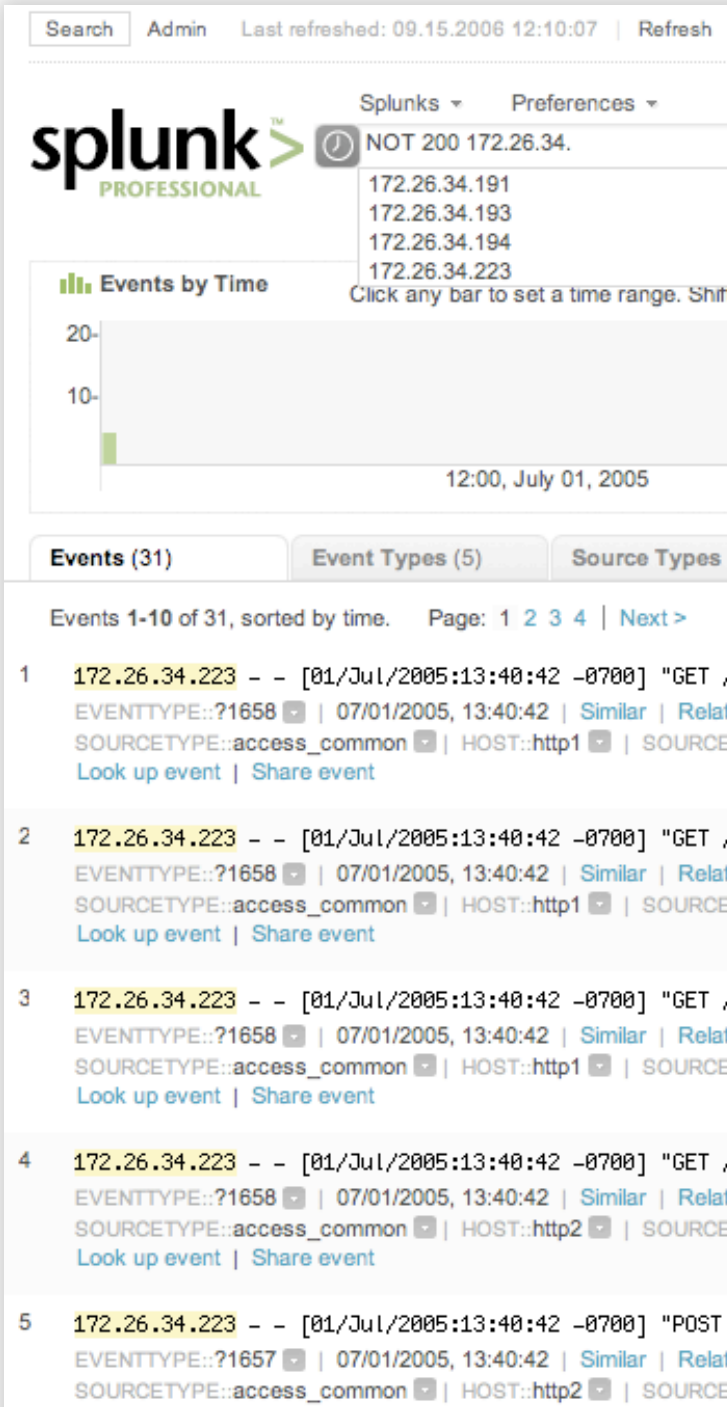
Splunk. The search engine for IT data.

Can you imagine trying to find things on the Internet without a search engine? Every day IT people face the challenge of trying to navigate terabytes of IT data logged by applications, servers and network devices. It's like trying to find a needle in a constantly changing haystack.

The Splunk Server is a high performance software server that indexes and enables system administrators, developers and even business users to search and navigate logs and IT data in real time.

- Achieve extreme availability
- Meet your compliance requirements
- Cut your operations costs

Cut incident response time and see multi-component problems before failures occur. Automate your compliance investigations, alerts and reports on user and system activities.



Powerful Interactive Interface

Get the big picture and dig deep with the intuitive AJAX user interface.

- Search for anything in the original data with powerful commands, booleans and type ahead.
- Interactive search results can be refined by clicking on anything in the results.
- Visualize trends and anomalies with interactive graphs.
- Navigate complex event relationships.
- Live Splunks alert you via Email, RSS or trigger shell scripts.
- Summarize search results with Report Splunks.
- Secure all your data with user-based access controls.

Universal Indexing

Your IT infrastructure and your IT data are always changing, so Splunk learns each type of source and different types of events on-the-fly. The more data you index with Splunk the smarter it gets. Data streams can be accessed from:

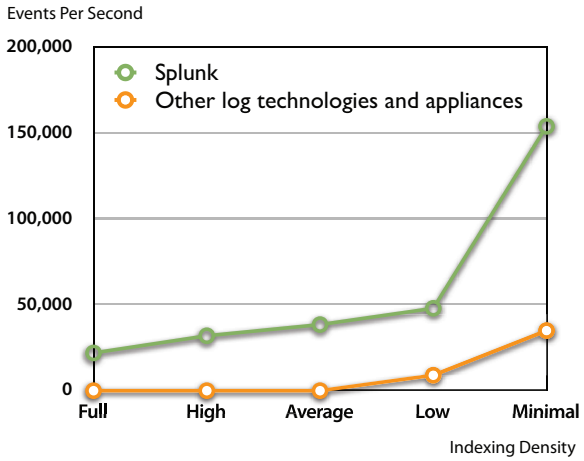
- **Mounted files:** NFS/SMB, CIFS/AFP, NAS/SAN, FIFO
- **Remote files:** rsync, scp/ftp/rcp
- **Network ports:** UDP & TCP, syslog/syslog-ng, log4j/log4php, JMX/JMS, SNMP
- **Databases:** SQL/ODBC
- **Custom APIs:** OPSEC LEA, CISCO RDEP
- **Splunk Servers:** Access data locally on production hosts and forward it to another Splunk Server over SSL/TCP.

High Performance

Splunk 2.1 is the highest performance technology for indexing, searching and managing logs and IT data. It delivers higher indexing throughput, faster search speeds and denser storage than previous Splunk releases and 3-5 times the performance of other log management technologies and appliances.

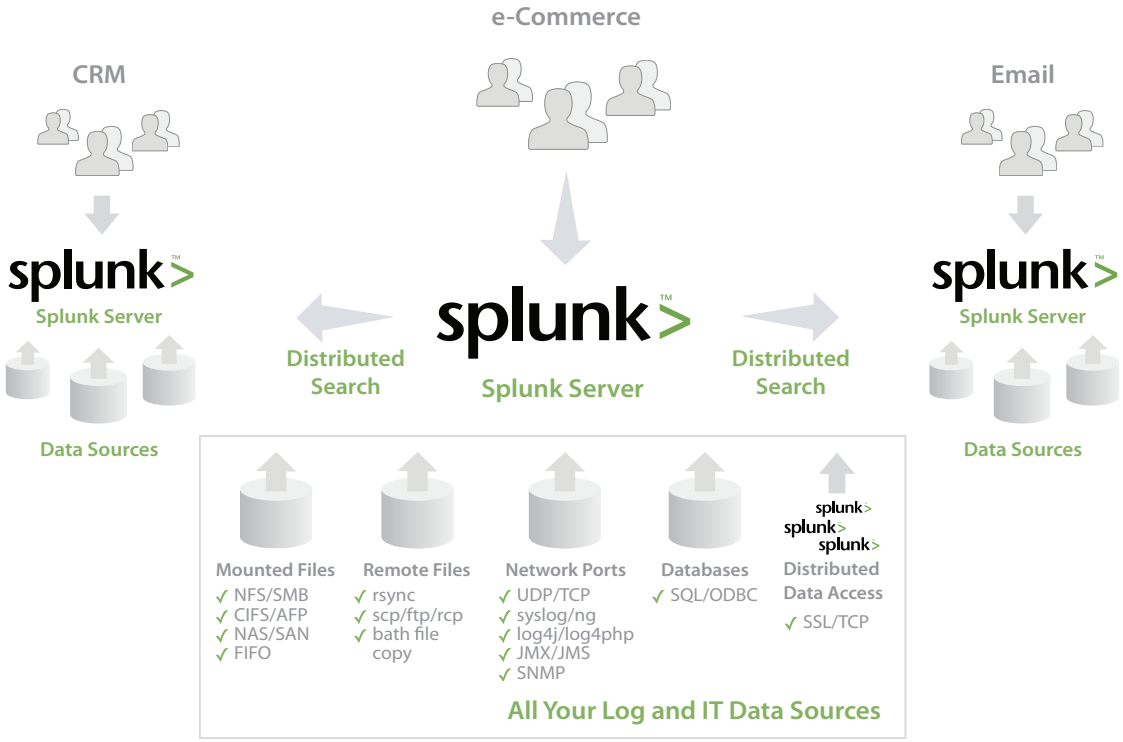
Index 3.3- 22.0 mbps (20,000-150,000 eps based on 150 bytes per event) on a single 2 x 3.0 gHz dual core CPU 4 GB RAM host.

Indexing speed varies based on configurable indexing density. Higher indexing speeds available by clustering servers together.



Scalable and Flexible

Deploy Splunk on a single server or across the data center to access, index and manage megabytes to terabytes of log and IT data each day. Splunk's distributed search feature lets you flexibly manage your data and search it in real time across application, technology and geographic silos. Splunk stores all your original data and the Splunk indexes in an efficient datastore engineered specifically for large-scale log and IT data.



System Requirements

Server Operating System

Linux (2.4-20 kernel+ glibc 2.3) / x86, AMD64, Xeon

Requires 32-bit compatibility libraries installed.

Solaris (8) / SPARC
Solaris (9, 10) / SPARC or X86

Free BSD (5.4, 6.0) / x86
Mac OSX (10.3+) / PowerPC or Intel

Server Hardware

1x 1.4 gHz CPU, 1 GB RAM (minimum)

2x 2.8 gHz CPU, 4 GB RAM (recommended)

Storage

12%-100% of the raw data size depending upon indexing density and type of data.

Supported Browsers

Firefox 1.0+ / Windows, Linux, and Mac

Netscape 7+ / Windows
Internet Explorer 5.5+ / Windows

Contact Us

Splunk Inc.
118 King Street
5th Floor
San Francisco, CA 94107
1.866.GET.SPLUNK
www.splunk.com