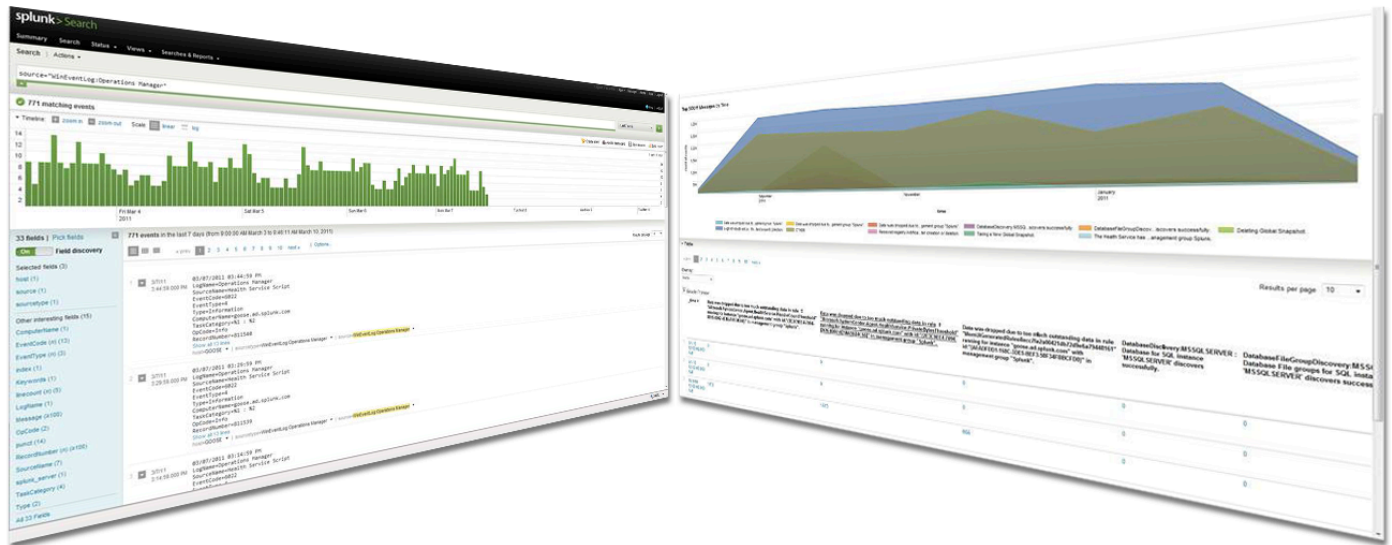




Splunk for Windows

Gain crystal clear visibility of your Windows environment.



Windows Has Never Been Easier with Everything in One Place

Splunk is the machine data engine that centralizes and indexes all the data generated by Windows desktops, servers and applications including event logs, registry keys, performance metrics and application logs in order to:

- Derive operational intelligence by monitoring and auditing usage of Active Directory, SharePoint, Exchange and custom applications
- Support regulatory compliance and security forensics with easily customized reporting and dashboards
- Speed mean time to recovery (MTTR) by up to 90% with real-time search from a single place across all machine-generated data, including network, anti-virus appliances and other non-Microsoft technologies.

Drive efficiency by eliminating costly, redundant agents and silos of instrumentation and security data. Avoid downtime by enabling monitoring to easily adapt to new components and problems over time. Splunk complements Microsoft System Center Operations Manager and other Windows management tools with single-click investigation integration.

The Old Way

Limited view increases management cost.

Centralized Windows monitoring is limited to filtered alerts and minimal performance metrics. Agent-based monitoring can be effective when configured right, but it comes at a high management cost. To provide even a limited view of server operations, multiple agents need to be licensed and

Windows is a registered trademark of Microsoft Corporation in the United States and other countries. All rights are reserved.

run on the same physical server to meet different monitoring objectives from performance to change and security. Despite this monitoring tax, diagnosing server problems still requires directly accessing individual servers and desktops to view decentralized application logs, run perfmon and view event log and registries. And, then you're only getting a fraction of the story. What about all of the other IT elements within the stack or what if your app or workload is supported by multiple servers—let alone multi-tenancy?

The New Way

Machine data engine gives you the whole picture.

Splunk collects and indexes all machine data generated by your Windows desktops, servers and applications with just one forwarder and no data connectors. Troubleshoot, correlate and analyze everything in one place with Splunk's simple but powerful search language. No more logging into each server to see what's happening. Searches can be saved and scheduled as proactive alerts to improve monitoring coverage over time. Reports and dashboards let you keep watch across the servers you manage. Splunk slashes the time to find and analyze problems and eliminates the need to install and manage redundant agents.

Using Splunk for Windows Workloads

Troubleshooting

Splunk is the first and last place you or anyone else in your organization needs to go to troubleshoot any problem with Windows server or its myriad of workloads. Launch a Splunk search directly from any alert in the System Center Operations Console and in minutes get a complete view of all of the performance, event and configuration data for that

host and timeframe. Correlate with other events based on time, host, transaction IDs or other terms by simply clicking on results. Find the root cause fast—configuration changes, administrative events or excessive loads. Splunk indexes registry data and performance metrics alongside application log files and Windows events so you get the complete picture in one window. It's so easy and accessible that your tier 1 staff will be able to resolve more incidents themselves. And when issues are escalated to developers, they'll have access to the data they need in real time, without needing to log into production boxes or interrupt administrators to request access.

Monitoring

Splunk is the most versatile monitoring tool in your arsenal. Save any search and schedule it to run routinely and alert you based on the results. Because Splunk can search any kind of machine-generated data—from logs to configurations—you'll cover your entire infrastructure with a single tool. Alert whenever a key configuration changes. Alert whenever a message shows up in a log. Alert whenever the number of transactions rises above a threshold.

Splunk won't become yet another console you have to watch. You can configure Splunk to send alerts via an RSS feed, email or forward alerts to the Systems Center Operations Manager console. Splunk helps you improve your monitoring over time. When you troubleshoot a new problem, you can immediately save and set up an alert on a recurrence of that event, transforming your monitoring from reactive to proactive.

Change Detection

With Splunk, you can continuously monitor files, registry keys and even Active Directory meta-data—without deploying yet another agent. Splunk records events every time a file, key or schema is added, changed or deleted. Splunk can index a snapshot of the entire file every time it changes, thereby giving you before and after states. Already have a dedicated change monitoring tool deployed? No problem. Just use Splunk to index events instead of monitoring for change directly.

Regardless of the source, with change data in the index, you can alert on changes to critical configuration settings and easily trace the root cause of errors to configuration changes.

Service Level Management

Splunk gives you the power to understand real service levels by leveraging the data already logged across all of your applications and components. There's no need for new instrumentation. Report on errors, transaction performance, and other metrics and drive dashboards for business owners, IT managers and customers.

Features

Splunk comes with pre-defined reports, alerts, searches and dashboards for better Windows management.

Index

- Indexes all the machine-generated data directly on Windows hosts including registry keys, the event log, perfmon and application logs WMI support for agent-less remote indexing of the event log and performance data.
- Splunk doesn't require a schema, obviating the need for data connectors.
- Universal Forwarder allows Splunk to deploy one forwarder on any OS, including Windows, providing even greater flexibility to Splunk's architecture.

Search

- Search the entire infrastructure from one place Launch searches directly from the Systems Center Operations Manager 2007TM console.

Alert

- Turn any search into a proactive alert.
- Alert via email, RSS or send alerts to Systems Center Report.
- Predefined and ad-hoc reporting and dashboards on performance data, utilization, activity and errors.

Share

- Easily customize reports to provide views for business decision makers, security practitioners and IT professionals.

Scale

- Splunk's architecture and licensing model use a scale-out philosophy, making it very easy to scale Splunk from monitoring a laptop to coordinating distributed searches across multiple datacenters.

Secure

- Secure, policy-based remote access to IT data enables stricter production controls.

Performance

- Splunk's Universal Forwarder collects performance data directly from Windows server, mitigating management cost while gathering highly granular data.

Get Started Today !

- Website:** www.splunk.com
Address: 250 Brannan St, San Francisco, CA, USA, 94107
Email: info@splunk.com | sales@splunk.com
Phone: +1 866-438-7758 | +1 415-848-8400
Free Download: www.splunk.com/download
Community: Splunk Answers | community@splunk.com