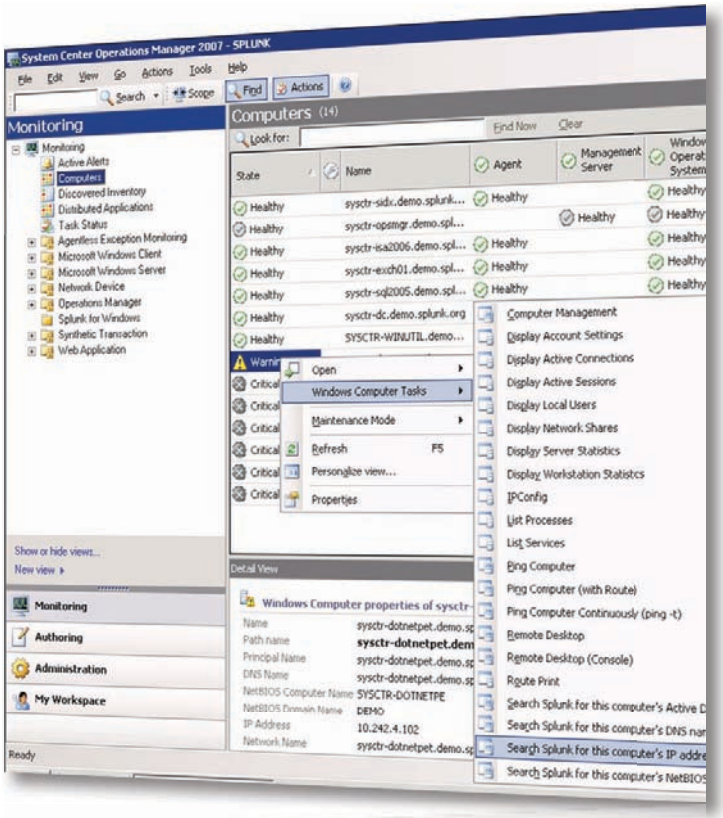
splunk>

Splunk for Windows™

Multiple agents are costly to deploy and still leave you in the dark.
Splunk simplifies Windows monitoring, troubleshooting, security and compliance.



Windows has never been easier with everything in one place

Splunk for Windows, an application built on the Splunk IT Search platform, indexes all the data generated by Windows desktops, servers and applications including event logs, registry keys, performance metrics and application logs

- Integration with System Center Operations Manager 2007 provides single-click search from the MOM console
- Pre-defined searches, alerts, reports and dashboards to accelerate Windows management tasks

Speed mean time to recovery (MTTR) with real-time search from a single place across all IT data. 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.

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 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.

The new way

IT Search gives you the whole picture.

Apply powerful searching, alerting and reporting to the challenge of managing Windows. With Splunk you can collect and index all IT data generated by your Windows desktops, servers and applications. Search everything in one place. 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

Troubleshooting

Splunk is the first and last place you or anyone else in your organization needs to go to troubleshoot any Windows server problem in minutes. Launch a Splunk search directly from any alert in the System Center Operations Console to 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 load. 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 IT 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. Best of all, 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, so you get notified by Splunk before another customer complains.

Change Detection

With Splunk, you can continuously monitor files and registry keys without deploying yet another agent. Splunk records events every time a file or key is added, changed or deleted. Splunk can index a snapshot of the entire file every time it changes. 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 for Windows provides two-way integration into System Center Operations Manager 2007 and comes with pre-defined reports, alerts, searches and dashboards for better Windows management.

Index

- Indexes all IT 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

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

- Everyday use captures knowledge of senior staff

Scale

- Deploy on one server with agent-less WMI data collection or scale across servers and data centers

Secure

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

Get Started Today !

- Download your own free copy of Splunk today at www.splunk.com/download.
- Download a 30-day free trial of the Splunk for Windows application at www.splunk.com/goto/apps/windows
- Visit www.splunk.com/goto/windows for tips, tricks and applications to help get off the ground with Splunk for Windows.