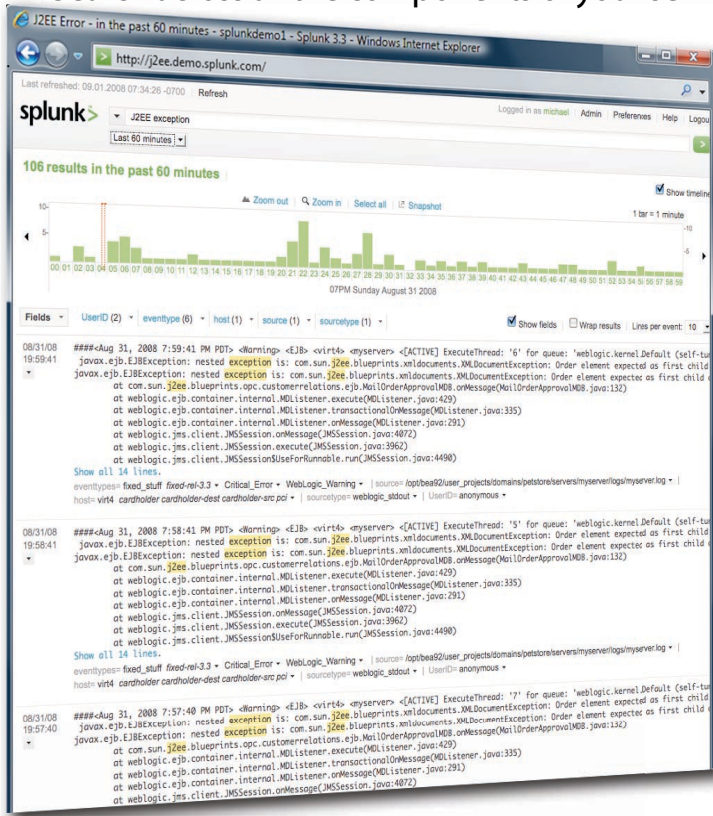


Splunk for Operations

Silos of instrumentation and tools slow the discovery of and recovery from problems. Search across all the components of your services from one place to find and fix problems fast.



Focus on Services not Silos

Splunk IT Search is the scalable, versatile way to keep up with all the complexity and change in your datacenter. Turn your silos of instrumentation from applications, operating systems, servers, networks and databases into integrated actionable information to improve mean time to recovery (MTTR) and keep critical services running.

- Applications
- Servers
- Messaging
- Networks
- Change Management
- Virtualization

Faster MTTR means less downtime and better service levels. Identify problems before your customers do. Splunk will be the first and last place you go to troubleshoot any service problem in minutes. Schedule searches to proactively monitor recurring problems. Provide simple form searches that empower front-line staff to answer routine questions eliminating costly escalations. Transaction searches and reports let you understand real service levels and deliver actual service-level reporting.

The old way

Silos of instrumentation slow recovery.

As the IT infrastructure has evolved, it's become so complex, dynamic, service-oriented and mission critical that it's hard to keep up. Multi-tier, scale out infrastructures, virtualization, service-oriented architectures (SOA) and composite applications create ever more complex and dynamic dependencies. The assumptions many tools need to make about service dependencies are out of step with the reality of constant change. Finding and fixing the problem takes too long and costs too much.

The new way

All your IT data in one place speeds recovery.

Index every type of IT data from every source and search, alert and report in real time across your entire IT infrastructure. Splunk consolidates data from multiple tiers, technologies and architectures. And with real-time indexing and search keeping up with virtualization and dynamic virtual machines isn't a problem. Finding and fixing problems faster means less downtime and improved service levels and performance.

Using Splunk for Operations

Applications

Complex distributed applications introduce many points of failure. Problems are hard to find and fix, delaying incident response and creating costly escalations. Application developers and administrators don't have direct access to the IT data they need. The resulting downtime impacts operations, revenues and employee productivity.



"Thanks to Splunk, our application issues are identified and resolved before they become problems that affect our systems, transactions and customers."

Robert Reilly, Sr. Manager Systems Eng, FreshDirect

Splunk helps you find and fix application problems fast. Search your entire application stack from one place to eliminate direct access to production servers for both production and non-production staff.

Change Management

Unauthorized change is a primary cause of downtime. Change control, CMDB and provisioning tools only cover part of your infrastructure. The lack of integration between change audit and incident management processes creates confusion. And unauthorized changes still go undetected.



"We use Splunk for our change monitoring requirements. Splunk's change management application does this more efficiently and with better functionality."

Joshua Edmonds, System Admin, Monash University

Splunk links change to system behavior. Search, alert and report on unauthorized changes across file systems, server and device configurations, logs and events and help desk tickets. Integrate change detection, reporting and validation with incident response.

Messaging

The complexity of messaging systems is massive. From tracing email messages and troubleshooting delivery problems, to managing compliance and analyzing spam and phishing attacks; the infrastructure is complex and resource intensive.



"Splunk empowers our frontline IT staff to instantly trace the path of lost messages across our Sendmail and Exchange infrastructure."

Yonas Hambissa, System Administrator, Interwoven

Splunk helps you search messaging transactions in real time across: activity logs, metrics from mail transfer agents, filtering and scanning devices, authentication and encryption technologies, firewalls and network devices.

Networks

In today's converged network infrastructures many network issues go undetected until it's too late. Errors and warnings buried in logs are ignored because of overwhelming volume. Writing scripts to analyze raw data is difficult and brittle as verbosity levels and data formats change.



"Splunk gives our customer service, NOC staff and network engineers comprehensive real-time event data for incident response, chronic problem identification and optimization."

Dave McCallum, Network Platform Architect, BT Design

Splunk lets you search, alert and report on network events and transactions across the complete network stack. Navigate from symptom to root cause quickly with syslog, SNMP trap, configuration and netflow data all in one place. Find early warning signs of problems that go undetected with component monitoring and integrate Splunk into existing network monitoring consoles for one-click investigations.

Servers

Server management costs are being driven sky high. Central server management is challenging, requiring many agents to grab data from the same server. Identifying and diagnosing server problems involves direct access and interfering with running systems.



"Splunk cuts down on the time to identify and investigate our server problems and outages by providing central access to all our IT data."

Andre Kocher, Sr. Systems Engineer, Swiss Post Finance

Splunk integrates logs, configurations, messages, traps and metrics all in one place. Search, alert and report across all your servers in seconds to troubleshoot problems, outages and chronic failures quickly. Integrate Splunk with existing server monitoring and provisioning tools for one-click deeper dives.

Virtualization

Virtualization brings more complexity and dynamic behavior to an already challenging IT landscape. Guest sessions fight for resources on the same physical hosts and performance can be unpredictable. Existing management tools can't keep up. And as guest sessions come and go the logs, events, messages and configurations disappear.



"Indexing both the physical and virtualized infrastructure enables end-to-end diagnostics and tuning. This is a requirement when you transition to virtualization."

Shaw Chaung, Former Director R&D, VMWare

Splunk provides visibility for the complete dynamic virtual stack. Search transactions spanning the virtual and physical components from one place. Splunk brings it all together for faster root cause analysis, security and compliance investigations.

Unified Communications

Unified communications demand a new approach to network monitoring. The slightest network hiccups can have far-ranging impact. Information is scattered and data sources are available through separate consoles, with no end-to-end reporting facility.



"Splunk for IT Operations provides unprecedented capabilities across increasingly complex UC (unified communications) environments."

Richard Whitehead, CTO, Clarus Systems

Splunk indexes data from every component in the delivery of unified communications services. Transaction search capabilities let you find and report across all events from all sources that relate to a single call or stream. Set up alerts when deliveries exceed quality thresholds to proactively identify problems rather than waiting for users to complain.

Features

- Index every type of IT data from any source
- Search your entire IT infrastructure from one place
- Distributed search across silos
- Turn any search into a proactive alert
- Report on performance data, utilization, activity and errors
- Adapt to change, no models or rules to maintain
- Everyday use to capture and share knowledge
- Integrate alerts with service desks
- Launch searches contextually from existing consoles
- Secure, policy-based access to IT data increases production control

Get Started Today !

Download your free copy of Splunk today at www.splunk.com/download.

Visit www.splunk.com/apps/ for tips, tricks and applications to help get off the ground with Splunk for Operations.