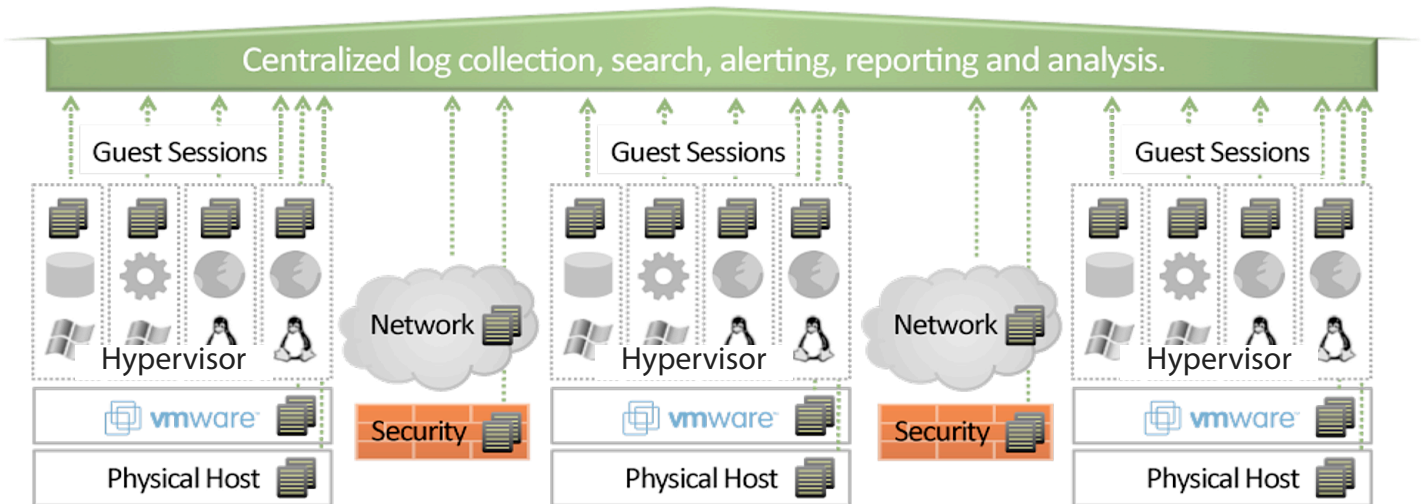


Splunk for Virtualization

Delivers visibility, proactive control and correlation across every layer of the virtual environment.
Scalable and extensible log and event management
for all elements of your virtual infrastructure.



End-to-end Visibility for Virtual Infrastructures

Splunk is the easiest, most scalable way to monitor and troubleshoot performance and availability issues across all layers of your virtual infrastructure, whether you have a few, or thousands, of VMs in your datacenter. Splunk IT Search lets you centrally search, alert, report and analyze logs and events across the complete virtual stack. Splunk gives system administrators and security analysts deep insights into the activities of applications, servers, virtual machines, hypervisors, operating systems, network devices, desktops, and security control points — all from one place.

- Proactively monitor your entire environment to detect performance degradation and prevent issues from impacting end users
- Determine root cause and fix issues faster
- Use Splunk searches, alerts and reports to understand the activities of every level of the virtual infrastructure in real time
- Easily collect, manage and correlate GBs to TBs of data from guest applications, OSs, hypervisors and physical network components
- Retain transient data from every element for root cause analysis, security and compliance

The dynamic and mission critical nature of today's datacenter requires real-time insight into and correlation of activities across every level and technology. Splunk provides a flexible, scalable solution for real-time collection and management of critical machine data from any component. Splunk correlates events across every level in the virtual stack with powerful real-time search capabilities. Flexible alerting and reporting provide continuous visibility into changing virtual environments. Whether you're testing a new virtualization rollout or managing an existing infrastructure, Splunk puts you back in control.

Using Splunk for Virtualization

Copyright© Splunk Inc. 2011 All rights reserved.

Log and Event Management

Splunk closes the gap in meeting log and event management challenges in virtual environments. Unlike traditional solutions, Splunk securely and remotely captures all your critical machine data in real time, even application logs from guest sessions. Now you can meet availability, security and compliance log and event centralization and monitoring requirements, including applications deployed on transient virtual machines.

Root Cause Analysis

When users call about performance or availability issues for virtual environments, Splunk is the answer. Most virtualization management tools focus narrowly on virtual environments and are unable to correlate events across different technologies in the virtual stack. In other cases, they require connectors, parsers for the different layers and are based on a filter and forward model, often lacking the ability to instantaneously drill down or flexibly run any kind of analysis.

Use Splunk to index machine data historically from all tiers. Then tie real application errors and performance problems to information about the state of the underlying hypervisor/OS/hardware. If the environment changed between the problem occurring and the investigation beginning, Splunk still indexed it and can help you solve it.

Take a common scenario: users complain about intermittent CRM app performance issues. Splunk can pinpoint the exact times and application server instances where performance fell below a threshold then correlate it with shared storage access issues captured from the virtualization platform logs.

Performance Monitoring

Splunk acts as a great monitoring tool since it indexes 100% of your machine-generated data—inside and outside of your virtual environments. You can schedule searches and alerts in Splunk to generate alarms on performance thresholds based on data gathered from the virtual machines, hosts and network interfaces.

Splunk also includes pre-built searches and reports for detecting key errors that indicate performance issues. Splunk can alert you when your VMs or guest OSs are short on free memory for too long. You can extend monitoring based on the outcome of root cause analysis: schedule alerts via email, warnings via RSS, or send events to consoles and ticketing systems.

Security and Compliance

Ensuring security and compliance, meeting audit requirements in complex, virtualized environments can be very challenging. Virtual machines and applications are not tied to a specific piece of hardware and generate massive amounts of log data that is required to be centrally controlled, managed and retained for differing periods of time.

Splunk helps you persist your log and event information at the required level of detail for security, audit and compliance regulations, for the requisite amount of time. It provides cradle-to-grave machine data management—collection, routing, retention, archiving and retirement. Splunk built-in, secure, role-based access controls allow a fine-grained granularity in moderating access to this data.

Splunk for Virtualization in Action

Splunk is widely deployed to manage hundreds and thousands of virtual machines, across multiple hosts and clusters, running a variety of different applications:

Splunk at a Leading Healthcare Services Provider:

“We thought we wanted a performance management tool – but really needed log management “plus” performance management to be proactive. Many tools can do performance management well, but that’s all they can do. No other product could pull VM host data, except Splunk.”

Joseph Rinckey, VMware Systems Engineer
Leading Managed Healthcare Services Provider

Splunk at a Leading Financial Services Provider:

“Splunk is the central console for our entire virtual environment – it’s our single go-to solution for troubleshooting any problem occurring in any layer of the environment.”

Systems Engineer, Large Financial Services Provider

Features

Only Splunk provides a unified view across virtualization platform metrics and configuration with the logs, configurations and metrics from guest operating systems and applications.

Index

- Remotely indexes all of the logs, metrics and configurations from all the applications and operating systems, hypervisors and the underlying infrastructure

Search

- Pre-defined searches accelerate troubleshooting across dynamic virtual environments
- Instantaneous free form search across all machine data across apps, guests, VMs, physical host and the network
- Find information hidden in logs without having to log in to multiple, individual hosts or virtual machines

Alert

- Pre-defined alerts notify administrators of common performance and resource contention issues
- Root cause investigation searches can be saved as new alerts to improve monitoring coverage over time
- Automated actions using management APIs

Report

- Pre-defined reports and dashboards provide management visibility into workload and service levels within virtualized environments
- Custom and ad-hoc reports can be created easily
- No schema to maintain. Identify fields and report on identified fields on the fly
- Persist transient data and flexibly report on it to meet compliance requirements

Share

- Users can collaboratively build and share knowledge about machine data unique to virtualized environments

Secure

- Fine-grained, role-based access controls easily audited
- Integrates with single-sign on infrastructure

Get Started Today !

Website: www.splunk.com

Address: 250 Brannan St, San Francisco, CA, USA, 94107

Information: info@splunk.com

Phone: +1 866-438-7758 | +1 415-848-8400

Free Download: www.splunk.com/download

Support: support@splunk.com

Community: Splunk Answers | community@splunk.com