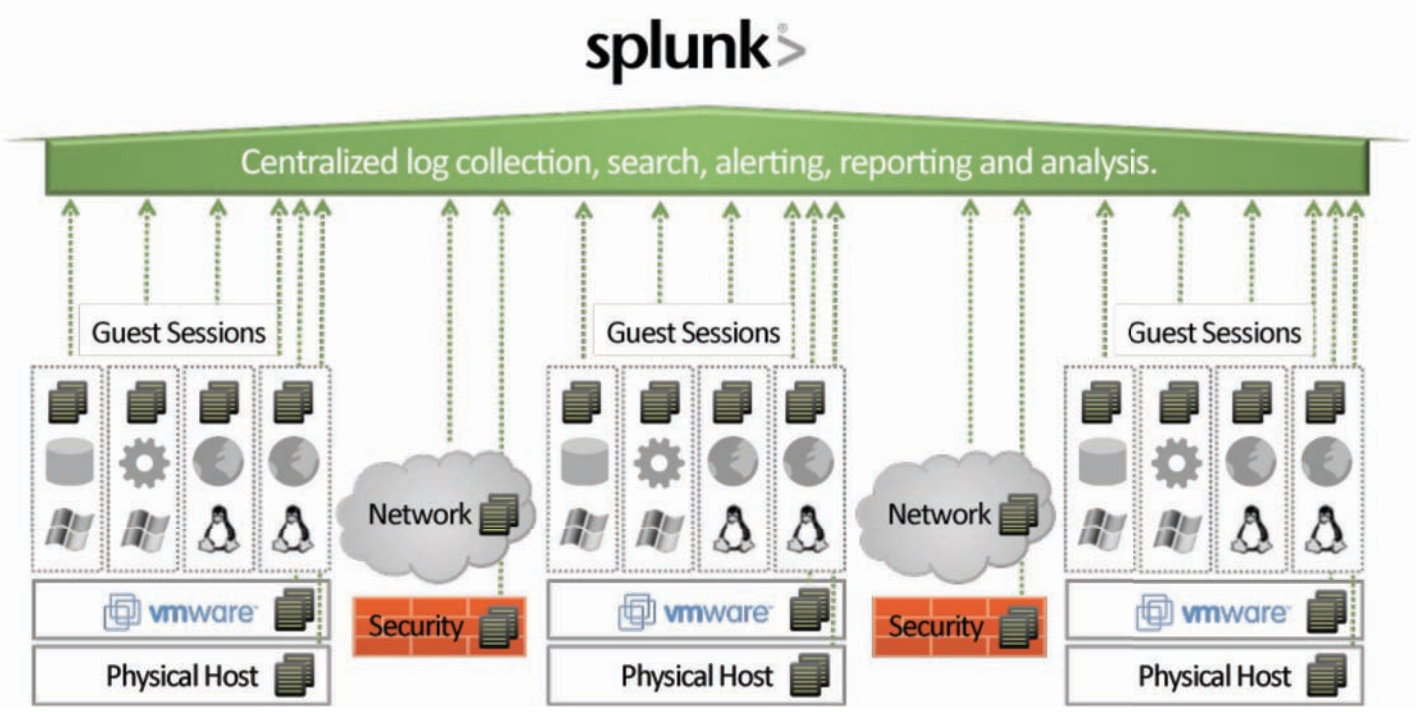
Splunk for Virtualization

Scalable and extensible log and event management for virtual infrastructures.
Delivers troubleshooting, security and compliance across every layer of the virtual environment.



Virtualization Log and Event Management

Splunk is the easiest, most scalable way to manage logs, messages and events across virtual infrastructures — regardless of whether you have a few or thousands of VMs in your datacenter. The Splunk IT Search engine 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 desktops, applications, servers, VMs, hypervisors, operating systems, network devices and security control points — all from one place.

- Use Splunk searches, alerts and reports to understand the activities of every level of the virtual infrastructure
- Search logs and events in real time from one place
- Easily collect, manage and correlate GBs to TBs of data from desktops, guest applications, OSs, hypervisors and physical network components
- Retain perishable data from transient guests for root cause analysis, security and compliance
- Simple search integration with leading virtualization management platforms

The dynamic, agile and mission critical nature of today's datacenter requires real-time insight into activities across every level and technology. Troubleshooting problems, investigating security incidents and meeting compliance data retention and reporting requirements demands the centralization of logs, events and other IT data.

The greater complexity of virtualized environments introduces new challenges to the real-time collection, correlation and analysis of critical IT data. The data is scattered across levels of technology and often lost as VMs are redeployed.

Splunk provides a flexible, scalable solution for real-time collection and management of critical IT data from any component. Splunk correlates data across every level in the virtual stack with powerful search capabilities that provide the visibility needed to troubleshoot problems quickly and achieve higher levels of availability. Flexible alerting and reporting provide continuous visibility and monitoring of changing virtual environments. Whether you're testing a new virtualization rollout or managing an existing infrastructure, Splunk puts you back in complete control.

Using Splunk for Virtualization

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 IT 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 even for applications deployed on transient virtual hosts.

Root Cause Analysis

Splunk is the answer when IT asks, "Where did that instance go?". Use Splunk to index IT data historically from all tiers as instances come and go to do root cause analysis. Then tie real application errors and performance problems to information about the state of the underlying VM and other guests. Even 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 configuration history captured from the virtualization platform APIs. Now you know which other guests shared the same physical hosts, can identify the I/O utilization hog, and even trend the I/O utilization of all of the guests over time.

Performance Monitoring

Splunk acts as a great monitoring tool since it indexes 100% of your IT 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 VMware API, Citrix Xen Management API, Hyper-V API about the guests, physical hosts and virtual and physical network interfaces. Splunk also includes pre-built searches and reports that monitor key virtualization metrics. 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.

Virtualization Planning

Splunk helps with planning even before the first hypervisor is loaded. Use Splunk reports for historical app and OS activity and utilization to identify good targets for virtualization. Splunk shows you a historical view of the apps with spiky workloads and the hosts with underutilized available resources, helping you marry the tasks and resources faster, instead of guessing through your first deployments.

Features

Only Splunk provides a holistic view of activities across every level of your virtual infrastructure.

Log and Event Collection

- Remote collection all of the logs, events, messages and configurations from applications, OSs, network devices and security control points
- Connects to VMware, Citrix XenServer and Hyper-V Management APIs to collect logs, metrics and configuration data

Search

- Ad-hoc search accelerates troubleshooting across dynamic virtual environments

Alert

- Searches can be saved as alerts for cross-component monitoring and to notify administrators of common performance and resource contention issues
- Alerts can trigger automated actions using management APIs

Report

- Reports and dashboards provide visibility into availability, security and compliance activities across every level of your virtual environment
- Ad-hoc reports can be easily created
- No database schema to maintain

Share

- Users can collaboratively build and share knowledge about the virtual environment

Secure

- Access control by role, user and type of data

Get Started Today !

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