The Virtualization Problem

While virtualized environments are significantly more cost efficient than traditional IT infrastructures they are also very complex. Virtualization tiers introduce additional layers of abstraction in datacenters making problem investigation, resolution and avoidance difficult. Existing IT management technologies either offer inadequate insights into virtual environments or provide a limited view and focus solely on the virtualization layer. Most of them also cannot collect or store performance data at full fidelity due to storage limitations and the inability to scale. As a result, many problems in virtualized environments remain unresolved and therefore keep recurring.

Enter Splunk

Splunk® Enterprise™ is a scalable and versatile engine for machine data such as logs, performance metrics and events. It offers a unique approach to solving difficult problems in complex virtualized environments. Use Splunk to collect, index and harness the power of all your machine-generated IT data across your virtualized infrastructure including the hypervisor, guest operating systems, applications as well as the underlying server, storage and network devices. Splunk lets you:

• Centrally monitor and analyze metrics, logs and events in real time across the entire virtual stack
• Correlate and connect events across every level and technology with its powerful search language
• Proactively detect performance issues and prevent them from impacting end users
• Determine root cause of outages or performance problems up to 70% faster
• Retain transient data from every element for trending, historical analysis, security and compliance
• Flexibly address reporting or operational analytic requirements such as capacity planning, usage analyses and asset reporting in the continuously changing virtual environment
• Scale to handle big data problems faced by the largest datacenters, with its unique MapReduce-based, schema-less technology

Splunk App for VMware

The Splunk App for VMware unlocks the value of vSphere data such as performance metrics, logs, vCenter Server tasks and events. It enables:

• Correlation of virtualization data with data from other technology tiers. Find causal links between application performance issues and the underlying hypervisor, storage, networking and server infrastructure
• Granular performance management and analysis. Collect and persist deep granular performance data directly from the vSphere hosts and trace virtual machine performance from host to host to troubleshoot contention-related issues
• Complete operational visibility and capacity analytics. Find capacity constrained hosts, idle virtual machines, underutilized clusters, overprovisioned datastores. Trend performance statistics to find usage patterns and likely capacity bottlenecks
• Change tracking and asset reporting. Track detailed user-initiated changes, automated vSphere actions as well as report on inventory and status of virtual components
• Security reporting and monitoring. Monitor the environment for suspicious activity, user role changes, unauthorized access and more

Performance Analysis

Collect, retain and analyze performance data about hosts and virtual machines at the deepest level of granularity (20-second time intervals). Trace and analyze virtual machine performance data in full fidelity as they move from host to host. Identify issues relating to resource contention among virtual machines. Correlate application performance with host and virtual machine metrics to gain deeper insights into response times of your mission critical applications.

Capacity Reporting

Find stress points within your infrastructure. Identify hosts, clusters and virtual machines that are over or underutilized. Find datastores that are running out of capacity and snapshots hogging unnecessary disk space.

Security Monitoring

Use the vCenter tasks & events data as well as VMware ESX log data to identify who did what and when in your virtual infrastructure. Find suspicious role changes, unauthorized user actions, failed and potentially harmful logins.
Log Analysis
Browse and alert on errors occurring in ESX, ESXi and VC logs to identify issues related to storage access, duplicate IPs, virtual machine connectivity and more.

Change Tracking & Asset Reporting
Track and report changes to virtual infrastructure components for troubleshooting and compliance analyses. Provide reports on virtual infrastructure assets belonging to various business units and their usage.

Customers Using Splunk & the Splunk App for VMware

Operational Intelligence About Your Cloud
CloudShare, a cloud computing service provider uses Splunk across their entire infrastructure for monitoring, troubleshooting, solving customer service issues as well as for operational intelligence about their business—understanding capacity usage per customer, conversion funnels and more. The Splunk App for VMware provides CloudShare added visibility into the detailed performance of their virtual infrastructure, helping them track stressed virtual machines and hosts to better re-balance capacity.

"Splunk gives us deep visibility and correlation across all tiers of our cloud infrastructure – giving us not only ongoing monitoring of key datacenter statistics, but also giving us business visibility into customer experience and usage"

Elad Gottfrid, Infrastructure Manager, CloudShare

Unprecedented Visibility
MelbourneIT uses Splunk and the Splunk App for VMware to retain a definitive record of everything that happened in their environment. They use it to trend and analyze performance as well as track user activities. Getting VMware data into Splunk meets several needs in their datacenter: operational monitoring, capacity usage, performance analysis and security monitoring.

"Using Splunk for VMware gets us all our data in one place, for many uses: capacity planning, event monitoring, performance analysis, security monitoring and more."

Peter Cole, Technical Lead, MelbourneIT

Rapid Troubleshooting and Analysis
Discovery Communications, the world’s largest non-fiction media company, uses Splunk to monitor application and operating system logs and events. The Splunk App for VMware enhances their operational visibility by giving them access to their virtualization layer data. With Splunk Discovery Communications gets an immediate understanding of virtualization layer failures and receives alerts before there is a full-blown impact on operations.

“I love that I can track virtual machines in my environment as they move from host to host. I can now identify the root cause of issues or errors”

Matthew Cluver, Network Operations Analyst, Discovery Communications

Product Requirements:
The Splunk App for VMware supports vSphere 4.x and vSphere 5.0. It works with Splunk Enterprise versions 4.2 and higher.

Free Download
Download Splunk. You’ll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. You can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

Splunk App for VMware – how to get it:
Please contact sales@splunk.com to get the Splunk App for VMware.