splunk>

FACT SHEET

Splunk® for VMware®

Cross-tier visibility and operational analytics
for your VMware environment

The Virtualization Problem

The rapid pace of virtualization adoption in the datacenter creates challenges for virtualization administrators. IT professionals have limited operational visibility into their virtual infrastructure, inadequate control over performance and security of virtual machines, insufficient insights into usage analytics and limited ability to compare virtualization performance to other IT layers.

Combating these virtualization challenges requires an approach that spans the virtualization layer and all other tiers of the infrastructure. The solution needs to provide actionable operational insights into performance, capacity, security and changes at the virtualization layer, in context of the other technologies in the IT stack.

Enter Splunk

Splunk® Enterprise is a scalable and versatile platform 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 software to:

- 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 a powerful search language
- Proactively detect performance issues and prevent them from impacting end users
- Determine root cause of outages or performance problems
- 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 a unique MapReduce-based, schema-less technology

Splunk App for VMware

The Splunk App for VMware harnesses the power of the Splunk Enterprise platform to provide end-to-end visibility and operational analytics for enterprise-class VMware deployments. The Splunk App for VMware is fast to install and scales to the largest of VMware deployments. The app provides real-time dashboards for immediate insights into the health of the environment. Users can accelerate troubleshooting by instantly detecting outliers and comparing performance events across a virtual topology map. Interactive dashboards allow you to investigate and discover problem sources, find resources that are over- or underutilized, track changes and detect security-relevant events. Execute blazing-fast queries on granular performance data over time for comprehensive pattern analyses, trending, usage tracking, forecasting and cost analyses. You can also gain real-time visibility into storage systems with direct drill down into NetApp Data ONTAP storage. Splunk Enterprise gives you a scalable big data platform to correlate data from VMware with other technology tiers, enabling faster problem resolution, flexible and powerful analytics, and end-to-end visibility across your IT operations.

Key Product/App Benefits

- Visualize the operational health of your VMware environment with immediate detection of underperforming/distressed hosts, VMs and data stores (see *Figure 1*)
- Access interactive, visual maps highlighting problems and statistical comparisons based off pre-defined, customizable thresholds
- Instantly identify outliers on a statistical map of your VMware environment
- Accelerate troubleshooting, optimize capacity and streamline workloads with out-of-the-box correlation between VMware and storage systems, including in-depth investigation into NetApp Data ONTAP storage
- Forecast future CPU, memory and disk requirements for VC, ESXi hosts and VMs using various predictive algorithms; analyze resource utilization and optimize capacity for cost benefits
- Gain visibility into potential security incidents and non-compliant usage patterns
- Explore unique errors and exceptions by relating granular performance metrics with VC and ESXi log data within a single console
- Track changes with visibility into vCenter tasks and events in the context of your virtual environment performance metrics, logs and topology
- Correlate data from virtual infrastructures with data across your entire IT stack for end-to-end visibility

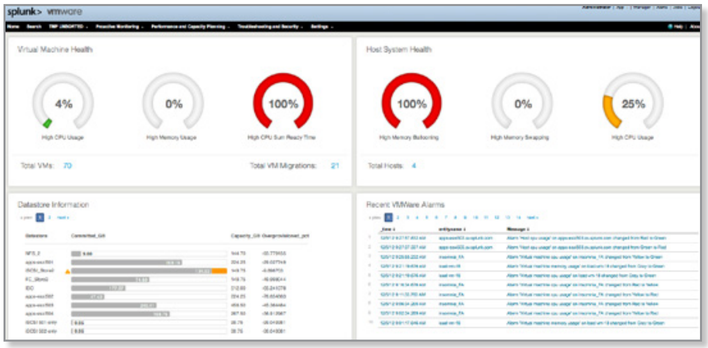

Figure 1: Operational performance insights across your VMware environment.

Features:

Health Summary

Get immediate visibility into the workload and health of your VMware environment. Identify which VMs are waiting on CPU or memory resources, determine hosts that are over- or underutilized, which data stores are running out of capacity and immediately identify problem areas.

Log Analysis

Analyze complete ESXi and VC log data, captured over syslog, for faults, security, changes and compliance issues. Investigate unique errors and exceptions related to storage access, duplicate IPs, virtual machine connectivity, iSCSI errors and more.

Change Tracking and Asset Reporting

Get a snapshot of all changes, tasks and events that were performed in your VMware environment and analyze the impact on performance, security or availability. Provide reports on virtual infrastructure assets to various business units and their usage for cost tracking and charge-back.

Interactive Topology Views

Use a visual interactive map of your VMware topology to gain immediate insights into the health of individual nodes (clusters, VCs, hosts or VMs) based on pre-defined thresholds. Instantly detect outliers, visualize trends and compare virtual entities and performance metrics to understand patterns over time.

Capacity Reporting

Proactively set alerts for real-time capacity monitoring so you can assess capacity risk. Optimize your resource utilization by establishing baselines, understanding capacity usage, trending analysis, and identifying capacity shortfalls. Forecast CPU, memory and disk capacity needs and performance levels of hosts, VMs and data stores by trending historical resource utilization data.

Security Monitoring

Use vCenter task and event data, as well as ESXi log data, to identify who did what and when in your virtual infrastructure. Find suspicious user activity, track potential attacks and audit user initiated changes. Report on user and configuration changes that can negatively impact security and proactively restrict and secure your virtual environment.

Correlation Across Virtual and Physical Infrastructure

Combine your virtualization data with data from all other technology tiers such as applications, operating systems, storage, networks and servers to gain a complete, central view of KPIs of your datacenter. Identify under- or overutilized storage resources, disk IOPS by ESXi hosts/VMs and discover hidden performance problems and capacity constraints.

Customers Using 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 and 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.

cloudshare

"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

Melbourne IT 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 to track user activities. Getting VMware data into Splunk meets several needs in their datacenter: operational monitoring, capacity usage, performance analysis and security monitoring.

MELBOURNE IT

"Using the Splunk App 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, Melbourne IT

Rapid Troubleshooting and Analysis

Discovery Communications, the world's largest non-fiction media company, uses Splunk software 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.

Discovery COMMUNICATIONS

"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 4.1 and higher. It works with Splunk Enterprise versions 6.0 and higher.

Free Download

Download Splunk for free. You'll get a Splunk Enterprise 6 license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

A 60-day free trial of the Splunk App for VMware is available at http://apps.splunk.com/app/725/