

# Splunk App for VMware

Gain Deep Insights into Virtual Environments with Correlation Across the Application, Hypervisor and Hardware Tiers

## A “Virtual” Problem

Virtual environments have proven to be more efficient but have added significantly more complexity to today’s datacenters. Abstraction of applications from the underlying hardware means that problems are harder to pinpoint and resolve—shared hardware also means shared problems.

Existing IT management technologies either provide inadequate visibility into virtual environments or are solely focused on the virtualization layer. With either direction there’s a gap tying together events from across different tiers of the infrastructure.

## Enter Splunk

Splunk Enterprise lets you easily monitor and troubleshoot performance and availability issues across the layers of your virtual infrastructure, whether you have a few virtual machines or thousands of VMs in your datacenter. Splunk lets you:

- Monitor, alert, report and analyze metrics, logs and events from a single location across the complete virtual stack
- Detect performance loss and prevent issues from impacting end users
- Gain real-time insight into and correlation of activities across every level and technology
- Determine root causes of outages or performance problems up to 70% faster
- Retain transient data from every element for root cause analysis, security and compliance
- Deliver on reporting or analytic requirement in the changing virtual environment

Whether you’re testing a new virtualization rollout or managing an existing infrastructure, Splunk puts you back in complete control.

## Using Splunk for VMware

### Root Cause Analysis

When users call about analyzing performance or availability issues for virtual environments, Splunk Enterprise is the obvious choice. Most virtualization management tools focus narrowly on virtual environments and are unable to correlate events from different technologies in the stack. In other cases, they require connectors or parsers for the different layers, a filter and forward model, retaining a fraction of the source data and lacking the ability to drill down or perform any ad hoc analysis.

Use Splunk to index machine data historically across virtualization 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 the issue.

Take a common scenario: users complain about intermittent CRM app performance issues. Splunk can pinpoint the 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 can index the machine data across your infrastructure—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, hypervisor, servers, storage and network interfaces.

Splunk also includes pre-built searches for detecting key errors that indicate performance issues and key reports that give you insights into the state of your virtualized environment. Splunk can alert you when your VMs or guest OSs are short on free memory for too long. Splunk reports indicate when virtual machines are waiting for host CPU time for too long or for memory to be available. 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 and 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 must 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’s built-in, secure, role-based access controls allow for fine grained granularity in moderating access to this data.

### 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 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 VMs.

**“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 Organization

## A Complete View of the Virtual Infrastructure

Only Splunk provides a unified view across virtualization platform metrics, tasks, events and logs, configurations and metrics from guest operating systems and applications as well as logs, events, traps and other data from the underlying network, server, and storage hardware.

The Splunk for VMware solution extracts data from VMware vSphere and vCenter and provides packaged searches that detect serious hypervisor level outages as well as views and dashboards that showcase performance metrics that are key to virtual environment performance.

## Features

### Index

- Remotely indexes the logs, metrics and configurations from 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 machine data: 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

“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

## Free Download

Download [Splunk](#) for free. You’ll get a Splunk Enterprise 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](mailto:sales@splunk.com).