07-12-2026

VMware

VMware is a global leader in cloud computing and virtualization technology, providing a wide range of software solutions that enable organizations to build, run, manage, connect, and protect applications across clouds and devices. Its core technology, the hypervisor, allows multiple virtual machines to run on a single physical server, optimizing resource utilization and operational efficiency.

Before looking at documentation for specific data sources, review the Splunk Help information on general data ingestion for Splunk Enterprise, Splunk Cloud Platform or Splunk Observability Cloud.

Getting data in

Source	Add-ons and Apps	Guidance
VMware With VMware, a hypervisor is installed on the physical server to allow for multiple virtual machines to run on the same physical server. Each VM can run its own operating system, allowing multiple OSes to run on one physical server. All the VMs on the same physical server share resources. To keep operations running smoothly, organizations that use VMware are interested in deep operational visibility into granular performance metrics, logs, tasks, events, and topology from hosts, virtual machines and virtual centers. In the Common Information Model, VMware data can be mapped to the Inventory and Performance data models.	**Splunk platform** • Splunk Add-on for VMware	**Configuration** • About the Splunk Add-on for VMware **Splunk Lantern Articles** • Monitoring VMware virtualization infrastructure • Monitoring VMware components with Infrastructure

Source	Add-ons and Apps	Guidance
		Monitoring
Indexes VMware Indexes refer to the structured storage and organization of data collected from VMware environments within the Splunk platform. These indexes facilitate efficient searching, reporting, and analysis of various VMware logs, metrics, and events, enabling users to gain insights into their virtual infrastructure's performance and health.	**Splunk platform** • Splunk Add-on for VMware Indexes • Splunk Add-on for VMware Metrics Indexes	**Configuration** • About the Splunk Add-on for VMware Metrics Indexes • About the Splunk Add-on for VMware Indexes
Metrics VMware Metrics encompass performance data collected from virtual machines, hosts, and other components within a VMware environment. These metrics, such as CPU utilization, memory usage, disk I/O, and network throughput, are crucial for monitoring system health, identifying bottlenecks, and optimizing resource allocation in virtualized infrastructures.	**Splunk platform** • Splunk Add-on for VMware Metrics Indexes • Splunk Add-on for VMware Metrics	**Configuration** • About the Splunk Add-on for VMware Metrics Indexes • About the Splunk Add-on for VMware Metrics
Extractions VMware Extractions refer to the process of parsing and normalizing raw log data from VMware environments into a structured format that can be easily analyzed by the Splunk platform. This involves identifying key fields and values within the logs to facilitate effective searching, correlation, and reporting for operational and security insights.	**Splunk ITSI** • Splunk Add-on for VMware Extractions	**Configuration** • About the Splunk Add-on for VMware Extractions

Source	Add-ons and Apps	Guidance
vCenter VMware vCenter Server is a centralized management application for the VMware vSphere environment, enabling administrators to manage virtual machines, hosts, and other infrastructure components from a single console. It generates logs related to tasks, events, alarms, and performance data, which are essential for monitoring, troubleshooting, and maintaining the virtual infrastructure.	**Splunk platform** • Splunk Add-on for vCenter Logs	**Configuration** • Splunk Add-on for vCenter Logs
ESXi VMware ESXi is a bare-metal hypervisor that serves as the foundation for VMware's virtualization platform. It directly interfaces with the server hardware to manage virtual machines, providing logs related to host operations, virtual machine events, and hardware status, which are critical for monitoring the stability and performance of the virtualized environment.	**Splunk platform** • Splunk Add-on for VMware ESXi Logs	**Configuration** • About the Splunk Add-on for VMware ESXi Logs
VMware Carbon Black Cloud VMware Carbon Black Cloud is a cloud-native endpoint protection platform (EPP) that unifies endpoint detection and response (EDR), next-generation antivirus (NGAV), and managed detection and response (MDR) capabilities. It provides advanced threat prevention, behavioral analysis, and continuous visibility to protect against modern cyberattacks.	**Splunk platform** • TA-VMware Carbon Black Cloud • IA - VMware Carbon Black Cloud • VMware Carbon Black Cloud	