Virtualization data

Virtualization data is a type of data that comes from software that is generally identified as a hypervisor. The hypervisor software allows a single physical computer to run multiple instances of an operating system, making it behave like multiple computers. These instances are called virtual machines. The main benefits are increased utilization of the underlying hardware and greater workload isolation. The hypervisor also simplifies and accelerates the provisioning of virtual machines (VMs) and allows for workloads to be moved from one physical machine to another without interrupting the work being done.

Functionally, a hypervisor is very similar to a traditional operating system as it presents a uniform interface to the hardware and coordinates the sharing of resources by the VMs. Example hypervisors are VMware ESXi, Microsoft Hyper-V, Xen, and Virtual Box. Virtualization has been around for a long time and is not limited to computation. It is also found in storage, networking, and application execution environments like Java and Python. This article, however, limits the source of virtualization data to hypervisors. In the Common Information Model, virtualization data is typically mapped to the Inventory and Performance data models.

Monitoring virtualization data is similar to monitoring OS related data in that we are interested in metrics such as cpu, disk, memory, memory management IO, and scheduling. Scheduling activity is very important because VMs share resources. All these metrics help identify how to keep loads balanced and can explain why certain VMs are not performing as expected.

Commonly monitored components in a hypervisor are:

- Inventory of hosts and guests (clustered)
- Location of VM on host
- Resource utilization
- Resource scheduling
- Virtual (V6I) Memory
- V6I cpu
- V6I IO (networking and storage interfaces)
- Filesystem and snapshot counts and sizes
- Hypervisor logs for tasks, events, and troubleshooting

Application

When your Splunk deployment is ingesting virtualization data, you can use it to accomplish security and compliance use cases.

- Monitoring VMware virtualization infrastructure

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
• Complying with General Data Privacy Regulation
• Verifying multifactor authentication usage
• Managing an Amazon Web Services environment

Sources

Guidance for onboarding data can be found in the Spunk Documentation, *Getting Data In* (Splunk Enterprise) or *Getting Data In* (Splunk Cloud). In addition, these Splunk Add-Ons and Apps are helpful for working with virtualization data.

• Splunk Add-on for VMware
• Splunk Add-on for Microsoft Hyper-V

Looking for more information on data types? Download the *Splunk Essential Guide to Machine Data*.