

What is Virtualization Monitoring?

 heroix.com/virtualization-monitoring

Virtualization monitoring ensures that a virtualized IT infrastructure performs optimally and that virtual resources are properly allocated. Virtualized infrastructure monitoring requires collecting and evaluating key performance indicators (KPIs) for both physical and virtual components. For example, VMware KPIs include:

- VMs
- Hosts
- Resource pools
- Datastores
- Clusters
- Data centers



Because physical resources are shared between VMs, problems that would be localized on a physical server can cascade through the virtualized infrastructure and compromise multiple applications. In order to cope with virtualization interdependencies, IT needs a monitoring strategy to optimize resource utilization by recognizing and reacting to performance and availability issues early in a problem cycle.

Find out how to make more cost-effective use of hardware, simplify disaster recovery, and properly size budget to need.

[Download the whitepaper: How Capacity Planning Can Optimize Your Virtual Resources](#)

Monitoring to Optimize IT

Monitoring a virtual environment differs from monitoring a physical infrastructure because there is no one-to-one correspondence between an operating system instance and a physical server. A typical virtualization host provides shared server, network, and storage resources for multiple operating system instances (VMs), each running their own OS and application workload.

In order to optimize IT in a virtualized environment, monitoring must encompass virtual resource utilization from the VM's perspective, application service levels, and physical resource utilization on the hosts.

Virtualization Monitoring Design

The following outline is a list of items to take into account when implementing a virtualization monitoring system:

How should you monitor?

- Automatically collect key physical and virtual performance metrics from hosts and VMs.
- Alert on potential performance or availability problems for both physical and virtual components and optionally take corrective action
- Generate comprehensive reports to show utilization and capacity issues for both physical and virtual components
- Correlate virtualization issues with end user response metrics for accurate assessment of application performance

What constitutes a problem?

- KPIs that exceed threshold values
- Alarms generated by virtual operating systems
- Misallocation of virtual resources: VM sprawl, too many VMs, or improperly provisioned VMs
- Poor application performance

What should you do when a problem is identified?

- Prioritize and escalate high severity alerts with text messages or email alerts
- For recurring problems build detailed notes into the alert to speed resolution
- For performance issues use reporting and capacity planning to better allocate virtual resources
- Automate with OS commands or scripts to fix the problem if possible

What are the benefits of reporting and capacity planning?

- Capacity planning with “What if” analyses predicts where and how potential changes (i.e. cpu and memory allocation) will affect operations and licensing costs Root cause analysis advances problem resolution
- Baseline of behavior based on function helps identify deviations from normal
- Reporting of availability and performance provides historical context



[Next Steps...](#)