



# Requirements for Virtualized Systems

## Virtualization Management RFP

Required Feature	Value of Feature	Additional Explanation
Access privileges	Basic security to prevent unauthorized people from accessing the hypervisors/VMS. Allows multiple roles to coexist on same invocation.	
Account for Colorblindness	Ease of use; meets Government 508 regulations	
Active Alarm Viewer	Centralized aggregation point for notification. Quick view of issues	All managed assets roll up into a single place for viewing alarms that actively get the latest alarm information
Alarm History or Log Files	Verification and audit trail of all activity on the system/history of what steps where taken to remediate problems in the past	System admins can know what was done on the system, when it was done, and who did it. Also, if a problem occurs admins can look back to see how it was handled in the past
Alarm or Incident Ownership	Call tracking	
App Manager and Agents Work on VM	Virtual Machine can be monitored and managed using the same tools and techniques that work on physical machines	
Application Monitoring	Applications running on the hypervisor/VM can be verified as to their availability and reliability	
Authentication	Allows system to be sure that people and machines are who they say they are	Prevents unauthorized access to critical resources
Control of Active and Passive Checks per Device	Keep out unauthorized people	
Customizable Dashboard	Customizable view that keeps the important information available at a glance	
Customizable Notification	Customizable way for alerts to get sent to admins	
Customizable Thresholds	Customizable number of occurrences in a given timeframe to produce alerts; values can be modified to meet changing environment	
Data Center Monitor	Management and monitoring of enterprise critical assets	
Device Mapping	Grouping of like assets	
Device or Inventory Lookup	Customizable identification tags for monitored devices to describe location/ownership of the asset	
Discovery of Network Elements	Active seeking out of all devices attached to the network	Depending on network configuration active discovery might not work or might only partially work with no warnings that the discovered device list is not complete
Easy Setup for Dependencies	Ease of use tools	
Efficient Client Application	Client application can co-exists with other running apps on an admin/user's workstation and not consume excessive network bandwidth	
Grouping of data inputs in Dashboard	Aggregation of data sources for "big picture" stats	Ease of use, quick understanding of issues
Limited UI access from a mobile device	Admins can have basic functionality for monitoring and management when "on the go"	
Log virtual machine	Record history of what happened on the VM, when it happened, and who connected to it	Increased value for signed log files that cannot be modified after the fact. Fills in gap from traditional log management systems that cannot log virtual machines.



# Requirements for Virtualized Systems

## Virtualization Management RFP

Required Feature	Value of Feature	Additional Explanation
Maintenance Tracking	Recorded notes from admins on system maintenance	Tracking of when systems were brought down, what was done - e.g. OS upgrade, hardware replacement, etc - and how long they were down
Manage XEN, VMware from same window	Admins can use the same tools from a single app instead of different tools from many apps	Less time learning and more consistent process
Minimal Footprint	Monitoring/management app should not effect the hypervisor or VMs that it connects to	Minimally invasive
Monitor Virtual Machines and Virtual Infrastructure	Alert and notify when errors are detected on VMs	
Multi-vendor server monitoring	Ability to manage, monitor the physical hardware as well as virtual components. Manage HP, IBM, DELL and other major vendor.	Sometimes the problem is hardware related, such as network card or storage device. Monitoring system must be able to see entire problem.
Must Run in a VM	Monitoring/management app can be run in a VM on an enterprise management hypervisor	
Network Monitoring	Problems with network equipment can be detected and analyzed	View of interconnectivity health
No Agents required	Agents are small software programs - managing the installation/updating/etc. of these small programs on all the equipment you want to monitor is error prone and difficult	
Notes Field for Alarms	Admins must be able to comment on what to do when a general alarm is triggered as well as what was done to handle a specific alarm	Follow-up and activity
On Demand Discovery	Admins can, when they want, discover the VMs that are running under a hypervisor	
Performance Monitoring	Monitors all manner of statistics of a machine including but not limited to CPU availability, disk io, network io, context switches, and memory usage	Important for provisioning and planning
Performance Reporting	Reporting and generation of alerts when performance data falls outside of an acceptable range	
Publish Reports	Save/print reports	
Remediate virtual machine problem	Solve problems that are detected on virtual machine	Enables large numbers of virtual machines to be monitored and remediated without having to have physical location with device.
Reporting Capabilities	Analyze/search log files to determine what/when happened	Good for forensic reporting.
Role Based Security	Allows different users/admins to only see those machines and operations that should be available to them based on their role - e.g. unix admin, windows user, etc.	
Scalability	Ability to add managed/monitored systems/hypervisors/VMs without loosing the ability to work with all the managed assets	Fewer invocations to manage.
Scalable to many sites	Ability to add systems from multiple physical locations	
SLA Aware Thresholds	Will alert when approaching an outage that violates a contract and/or causes punitive monetary payments	



# Requirements for Virtualized Systems

## Virtualization Management RFP

Required Feature	Value of Feature	Additional Explanation
SMI-S / CIM support	Storage Management Initiative / Common Information Model - managing devices that support an object based information model for querying/reporting the state of the device	
SNMP polling support	Simple Network Management Protocol support to query the state of a device	Support for older infrastructure standards
Trending (Graphing)	Analyze/view directions for monitored data	
Unique Alarm or Incident ID	Ability to provide a keyed identity to a particular alert	Using the key actions and comments can be tied back to the originating event/alert
Visibility to NAS	Must be able to monitor and manage the Network Attached Storage	
Visibility to SAN	Must be able to monitor and manage the Storage Area Network	
Windows Management Instrumentation (WMI) support	Must be able to manage/monitor Windows devices using the WMI protocol	
Common Information Model Object Model (CIMOM) Capable	Must be able to utilize latest industry Standards for Infrastructure Management to include virtualization	
Compatible with Open Virtual Machine Format (OVF)	Able to utilize latest industry Specifications on Open Virtual Machines - for management and configuration	