Virtual Certainty

Best Practices for Gaining Monitoring Clarity in VMware Environments

Nimsoft Whitepaper

Virtual Certainty

Table of Contents

Executive Summary 3
Introduction 3
Challenges of Monitoring Virtualized Environments 4
Best Practice #1: Get a Complete Picture of the Infrastructure 5
Best Practice #2: Automate Monitoring of VMs 6
Best Practice #3: Correlate Physical and Virtual Resources 7
Best Practice #4: Maintain Awareness with vMotion, HA, and DRS 8
Best Practice #5: Fully Integrate Monitoring with the Rest of the Infrastructure 8
Best Practice #6: Track and Communicate the Value of IT and Virtualization 9
Nimsoft: Optimizing Performance and Efficiency in Virtualized Environments 10
Conclusion 10

Virtual Certainty

Executive Summary

The benefits of virtualization are unassailable: increased agility, scale, and cost savings to name but a few. However, so too are the monitoring challenges posed by these environments—including complexity, lack of visibility and control, and inefficiency. This white paper reveals the best monitoring practices to employ in virtualized environments—best practices that are essential in enabling organizations to overcome their monitoring challenges so they can get the most business value from their virtualization investments.

Introduction

In just a few years, virtualization has ushered in a fundamental, pervasive paradigm shift in how IT services are delivered in enterprises. While in 2009, it was estimated 16% of IT workloads were running on virtual machines, that number is expected to climb to 50% by the 2012 . Further, it is virtualization that's helping fuel another game-changing trend, with virtualized systems at the foundation of both private and public clouds. When it comes to virtualization in the enterprise, VMware is the dominant, pervasive vendor, with a presence in 100% of the Fortune 100 and approximately 96% of the Fortune 1000 .

The increasing ubiquity and maturity of virtualized environments means that, not only are more applications running in virtualized environments, but more critical applications are running in them as well. While many businesses started virtualization initiatives with smaller, less critical applications and services, today some of the most transaction-intensive and business-critical services are running in virtualized environments. Now, in addition to file and print servers or development and test environments, business-critical Web property production instances, ERP systems, email, and other key services are running on VMware-powered infrastructures.

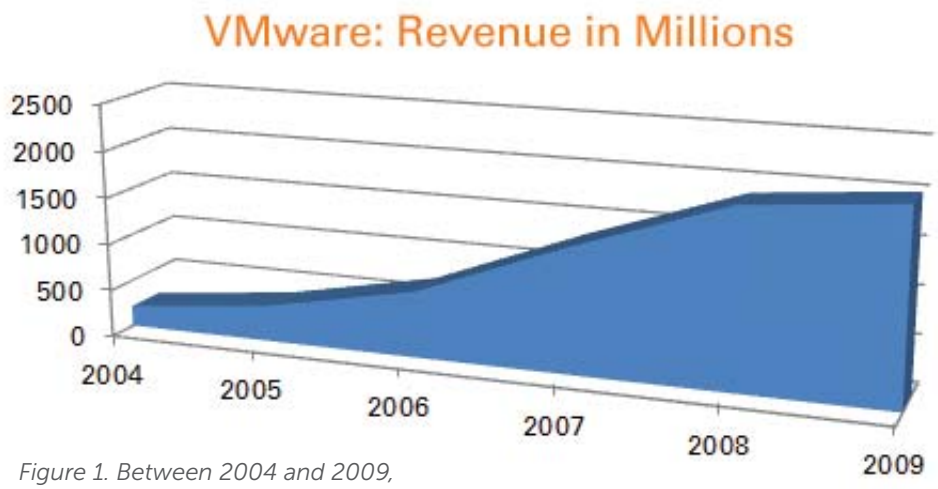

Figure 1. Between 2004 and 2009, VMware revenues have grown from $218 million to over $2 billion, with the company establishing a presence in 100% of the Fortune 100[2].

Consequently, doing effective service level monitoring in order to ensure optimal performance and continual availability is a vital mandate today. However, this demand for effective monitoring can't equate to manual, labor-intensive administrative efforts or many of the advantages that organizations seek to gain through virtualization will be negated.

Fueled both by virtualization's technological advancements and by increased competitive and pricing pressures in many industries, IT administrators' responsibilities have dramatically expanded in scope. Where in the 1990s, a system administrator may have been responsible for the management of ten physical servers, today, that same individual may oversee thousands of both physical and virtualized servers—with the expectation being that the number will continue to grow. Consequently, automation is essential to

scale administration and to effectively optimize performance of virtual environments.

Supporting virtualized environments presents a host of new monitoring challenges. Driven by the density and complexity found in virtualized environments, and the mission-critical applications that are being deployed there, monitoring must be aligned to support virtualization. Without effective monitoring, virtualization efforts will fail to fully deliver on their potential to provide businesses with such benefits as lower costs, flexibility, and agility.

Challenges of Monitoring Virtualized Environments

To understand the challenges of monitoring in VMware environments, it is important to start with a description of the complex ecosystem represented by these deployments. Following are the critical elements that factor into monitoring within VMware environments.

Solution layers:

- Virtual machine (VM) guests, which can be thought of as virtual servers that run on an ESX host.
- VMware ESX host, which is the server that houses one to many virtual machines.
- VMware vCenter server, which forms the foundation for virtualization management.

Scalability and availability elements:

- VMware vMotion, which is used to transfer virtual machines between physical servers on the fly. vMotion can take a VM running on an ESX host and move it to another host, perhaps so it can get more resources when it needs, or to constrain it from consuming too many resources.
- VMware HA, which is used to automatically restart VMs in the event of a physical or virtual server failure.
- VMware DRS, which dynamically allocates resources (such as CPU, memory, and disk) between VMs on a single physical machine. For instance, DRS may allocate more CPU to a VM running an application that is experiencing a spike in usage.

"In many organizations, administrators tasked with monitoring these environments have had to resort to using several tools to track performance of all the physical, virtual, and application level elements. This is not only expensive, but costly and complex to maintain on an ongoing basis."

Within this multi-layered infrastructure, there are a lot of "moving parts". Systems routinely come up and go down. The location of a given workload can change frequently, shifting both to different virtual and physical machines, with IP addresses changing routinely.

Further, underlying these virtualized systems are storage area network assignments, and physical and virtual networks. The processes and services that underpin the virtualized environment must also be adapted to the changes in the virtual realm. For example, if a blade in a rack of servers fails, the workload on that blade will need to be migrated onto another resource, and another new blade or other physical resource may need to be put online. Or, if a CPU on a VM-based server that is the sole tenant on a host reaches 90% usage, vMotion may automatically move the VM host to a server with twice the CPU resources, and then automatically move it back if CPU usage falls to 50%.

In many organizations, administrators tasked with monitoring these environments have had to resort to using several tools to track performance of all the physical, virtual, and application level elements. This is not only expensive, but costly and complex to maintain on an ongoing basis.

Further, even with multiple monitoring tools, identifying the source of issues in virtualized environments, let alone predicting and taking precautions to guard against potential issues, can be problematic. For instance, if a user is experiencing difficulty accessing an application, an administrator may need to check multiple systems and dashboards, and manually correlate the information gathered to identify the source of the problem. To find the source of an issue, an administrator may need to check many disparate tools in order to get answers to these types of questions:

- Is the application on the VM down?
- Has the network service in the guest VM failed?
- Is the VM guest OS operational?
- Is there a problem with the virtual network on the ESX host?
- Has the ESX host failed?
- Is the physical network adapter on the server operational?
- Is there a power or CPU problem on the physical server?
- Have the fabric interconnects to storage from the physical server failed?
- Is the storage that underlies the physical server operational?

As organizations continue to run vital business services in virtualized environments, while expecting administrators to manage an increasing number of resources in these complex environments, they need to apply a host of best practices for delivering, configuring, and using monitoring. The following sections outline these best practices.

Monitoring Converged Infrastructure Packs

In order to fully leverage the benefits of virtualization, many organizations are looking to build private clouds. However, designing, developing, testing, and implementing a private cloud may take considerable time, expense, and effort. Further, to develop these clouds, businesses must either reallocate existing infrastructure elements, or go through the process of architecture development, design, procurement, and implementation of all the hardware and software required. Consequently, converged infrastructure packs, such as Vblock and FlexPod, offer a very compelling solution. These converged infrastructure packs include everything an organization needs to deploy a private cloud, including servers, software, and hardware—all fully integrated and ready to plug in, with one purchase and one organization providing support.

Once deployed, however, organizations need to monitor and maintain performance of these converged infrastructure solutions, just as they would any other infrastructure component. Further, even with monitoring for each of the specific systems within these infrastructure packs, administrators will still be challenged, as with monitoring any virtualized environment. Gaining a cohesive, single view of these infrastructure packs grows more critical because a solution like Vblock 2 is capable of running 3,000 to 8,000 VMs—the equivalent processing power of an entire floor in a data center employing last-generation technology.

The extreme density of infrastructure packs' computing power, the virtualized nature of their resources, and the non- standard nature of their supporting hardware requires a different approach to successfully ensure organizations meet SLAs and uptime commitments of applications and IT services. To effectively run converged infrastructure packs, IT teams need a monitoring solution that covers all of the physical, virtual, and application layers; one that automatically discovers changes to resources; and one that automatically deploys monitoring, displays, and reports.

Best Practice #1: Get a Complete Picture of the Infrastructure

To effectively control virtualized environments, administrators need to gain a comprehensive, multi-layered view of the entire virtualized infrastructure—including physical systems, virtualized resources, and applications.

To illustrate, consider the following scenario. An administrator receives repeated calls from users, who claim that the internal banking application used to serve checking statements is "taking forever". The administrator has VMware vSphere running, which

offers basic monitoring of CPU, memory, disk, and network usage. Using vSphere, the administrator can see that the virtualized servers, which are running the multi-tier Web application that serves the checking statements, appear healthy. However, while disk, networking, and memory are all within their threshold limits, CPU usage is exceeding thresholds on several application servers. Given the fact that the application spans multiple tiers, including Web, application, and database servers, identifying the source of the issue can be a real problem. In order to find and fix the problem, the administrator needs to take a deeper look into additional layers of infrastructure:

A "noisy neighbor" located on the same physical server may be consuming all of the available CPU and causing the slowdown.

An Apache Tomcat server or WebLogic application server may be having issues due to a recent software patch—while OS, memory, and disk all appear fine, the required services are consuming more resource than expected.

- Center may be down or not be responding as expected, for example, not reallocating CPU with DRS when thresholds are hit, and so the resources the application requires aren't available.
- Networking bandwidth to the physical server may be constrained by other applications sharing the same resource.
- The problem might not be in the VMs experiencing high CPU usage at all, but in downstream access to a database cluster, one that resides outside of the virtual environment, that has failed and is in the midst of a rebuild.

In this scenario, an IT administrator cannot solve the problem with the simple tools available from VMware. The administrator may need to enlist the help of other domain experts and refer to a handful of tools, for example one for monitoring the network, one for vCenter, one for Weblogic, one for the database, one for the physical chassis and environmental state, and so on, to rule out all the potential causes of the issue. Even for experienced administrators, this process can be extremely time consuming, and delays could lead to downtime and have an array of other costs.

To be effective and efficient in these virtualized environments, administrators need to employ a solution that covers the entire infrastructure. They need to be able to quickly and easily view the current status of all points within the infrastructure, both to solve known issues and to spot trends and make corrections before issues arise.

Best Practice #2: Automate Monitoring of VMs

Given the dynamic nature of virtualized environments, businesses need to automate as much as possible. This is vital both to minimize administrative effort and to ensure monitoring information is sustained and meaningful. Following are the essential capabilities required to automate monitoring in virtualized environments:

- Automated discovery. Both physical and virtual resources may change often. For example, when a blade fails, HA may migrate processing to new locations. vMotion may move a VM to a new machine. Using a self-service portal, a user may start a new virtual server instance. In these cases and more, monitoring solutions need to automatically discover guests, and detect, register, and apply

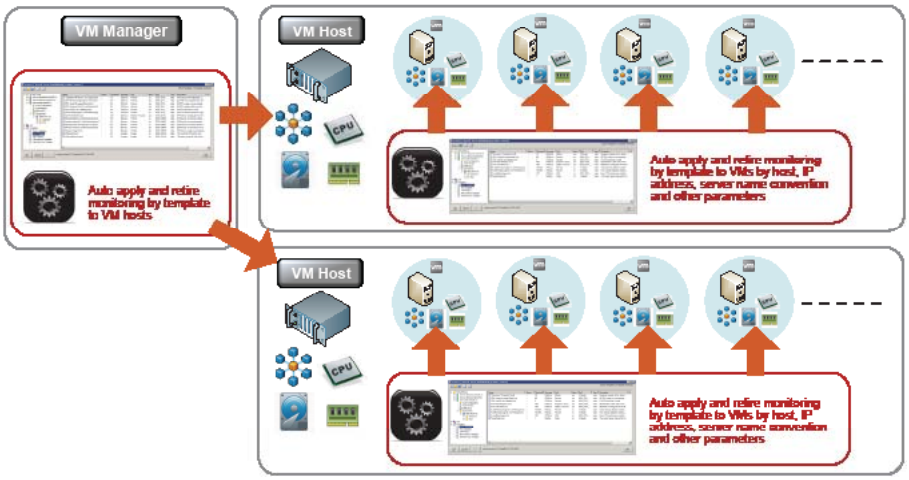

Figure 2. To meet performance and efficiency requirements, IT organizations need to automate the application and retiring of VM monitoring.

appropriate monitoring to them—as they are brought online.

- Agentless, automated monitoring via policy templates. Once resources are discovered, businesses need to use templates to automate the policy applied to them. These templates should assign the monitoring configuration of common items—including CPU, disk, memory, and network—and be able to apply them by the type and characteristics of the image. For example, a business could set up a monitoring template for email servers that would specify a network resource threshold of 60%. On the other hand, a database server template may specify a threshold of 90%. These templates should be used both for alerts and performance management or historical and trending data.
- Automated configuration and deployment of agent-based monitoring. When agent-based monitoring is required—for instance to monitor Web server processes on a VM instance or to deploy detailed database monitoring to new database servers—organizations need to configure and deploy agent-based data collectors automatically. To do so, administrators must integrate appropriate monitoring data collectors and their configuration with "gold master" VM images or through integration with provisioning systems and configuration management databases (CMDBs) that will dynamically create the VM instances.

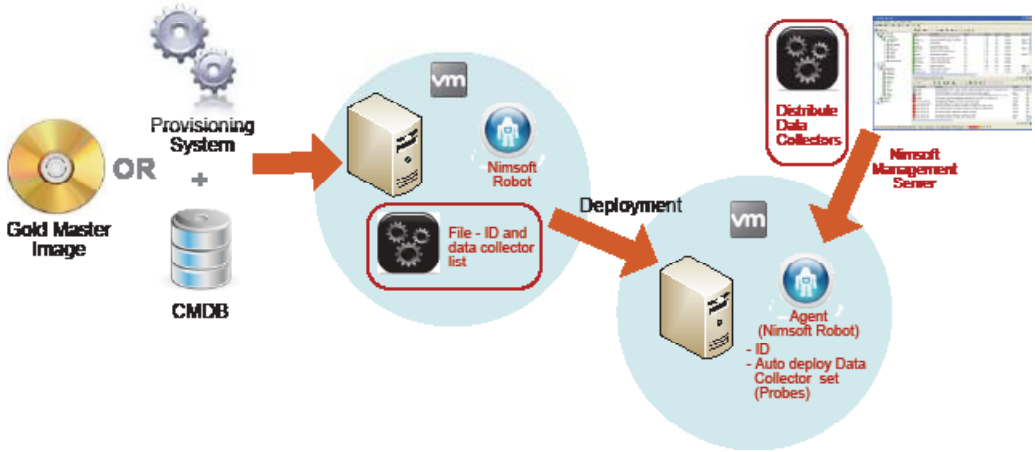

Figure 3. For agent-based monitoring, administrators must integrate appropriate monitoring data collectors and their configuration with "gold master" VM images or through integration with provisioning systems and configuration management databases (CMDBs)

- Automated display. Organizations also need to ensure that dashboards and reports are automatically populated with accurate, meaningful data. For example, data for a given instance needs to be properly associated with the right groups of physical servers and other resources. Further, if a VM is decommissioned intentionally, for example due to scheduled maintenance or a policy being implemented, reporting needs to have the intelligence to distinguish that occurrence from an unplanned outage, so a host of false alarms don't get generated.

Best Practice #3: Correlate Physical and Virtual Resources

To be truly effective in identifying and preventing issues and outages, administrators need to leverage capabilities for correlating the monitoring of physical and virtual layers. Following are some of the key requirements:

- Correlation between the ESX host and associated VMs. A business may have eight virtual hosts running on a physical blade

server, and an administrator may see that users are having trouble getting to applications running on those systems. In cases like these, administrators need to see whether the issue is being caused at the host, for example due to the fact that one of its network cards went down, or identify whether an issue arose that was specific to a single VM.

- Correlation with the physical layers underlying the ESX host. The performance of the ESX host is contingent upon a host of physical layers, including physical storage, such as storage area networks (SANs); networking devices; fiber connectivity; power; cooling; and more. Effective remediation and resource control requires administrators to be able to quickly assess the current status of all these elements.
- Correlation with VMs and resident applications. Administrators need to have visibility into the performance of VM-resident applications, including email servers, databases, packaged applications, and so on, which may span multiple virtual servers. Display and correlation of problems need to take an integrated view that covers the entire application as well as the underlying VMs and infrastructure.

Armed with these capabilities, administrators can be well equipped to make more sophisticated policies that enhance performance and maximize the utilization of physical resources:

- Under usage. An administrator may set a policy so that a resource owner is automatically notified if 2% or less of a VM is used over a two-day period. That way, the resource owner can determine whether to turn that VM off so resources aren't reserved unnecessarily.
- Over commitment. If one VM sitting on a physical host is taking 90% of the network resources available, other VMs sharing that host's resources won't have the performance desired. In these cases, administrators need to be alerted automatically, so they can determine whether there's a problem, and, if so, find out where. For example, a software issue may be creating high volumes of network traffic, usage and traffic may have spiked due to unexpected activity, or the ongoing commitment required for that VM may not have been forecasted correctly. Based on this understanding, the administrator can then take corrective action, such as fixing an issue or migrating other VMs to other physical machines.

Best Practice #4: Maintain Awareness with vMotion, HA, and DRS

As mentioned earlier, vMotion, HA, and DRS are the vehicles within VMware environments that automate the migration of resources. Following are a few practical examples:

- Mail server. An organization's server administrator may set up a policy in DRS specifying that, if the VM running the email server reaches or surpasses CPU utilization of 50%, that VM's allocation will go from 1 CPU to 3 CPUs. Further, the policy may specify that, if usage slips back to 25%, the allocation should go back to 1 CPU.
- Database. For VM-resident databases processing critical workloads, an administrator may dedicate only one or two VMs to a physical host. In this environment, if CPU utilization or network usage rises above specific threshold, the administrator can set a policy using vMotion to move the VM to another physical machine that has more CPUs and bandwidth available.
- Blade failure. If a fan in a chassis fails, causing a blade to fail, VMware HA migrates the workloads from that blade to other resources.

To monitor these environments effectively, administrators need to leverage monitoring solutions that have an integrated, synchronized awareness of these automation technologies. When vMotion, HA, and DRS automate the transition of a VM or process to another physical machine, the IP address will change. Another thing may be changed is MAC address. For example, when organizations use tools such as Dell's Scalent solution, workloads can quickly be migrated between virtual and physical machines. To monitor these environments effectively, administrators need to ensure monitoring can seamlessly, automatically

be updated to reflect these changes. Further, monitoring solutions need to be able to retain monitoring continuity and history, so administrators can better track and assess these issues over time and set better policies.

In virtualized environments, it is important for administrators to configure thresholds with percentages, rather than specific numeric figures. For example, vMotion may shift a VM from a machine where it is assigned 2GB of memory to another where it is assigned 8GB. In this scenario, if an administrator sets a memory utilization threshold of 700MB in the lower resourced system it will result in under-utilization when moved. Setting thresholds based on a percentage basis ensures the optimal policy regardless of which machine a VM is running from.

Best Practice #5: Fully Integrate Monitoring with the Rest of the Infrastructure

Because monitoring plays such a central, critical role, it is vital that businesses most broadly integrate monitoring into their IT infrastructure. This is key to both leveraging existing infrastructure investments and monitoring insights as fully as possible.

In many organizations, this integration needs to start with the management infrastructure. Organizations typically have existing service desk applications, CMDBs, and other IT infrastructure management tool investments, and the more virtualization monitoring can be integrated with these applications, the better and more efficiently they can run their IT operations. For instance, virtualization monitoring should be integrated with the organization's standard IT ticketing workflow in an existing service desk application, so that minimal changes to operating procedure are required. CMDB integration allows changes to monitoring requirements to be centrally maintained and implemented—enabling automated deployment and updates to supported configurations.

Further, this integration needs to be enabled at any layer in the monitoring solution stack, including the data, message bus, operations, and presentation layer. For example, at the presentation layer, a business may have dashboards in their service desk application, and may want to pull monitoring data from the virtualization environment to populate portions of those dashboards, allowing them to more efficiently manage ticket assignment and remediation efforts.

Following are additional opportunities for integrating monitoring with additional areas in the IT infrastructure:

- Provisioning, change, and configuration management tools. To streamline administration, an organization

Custom Environment Support

It is important for monitoring integration to extend to customized systems and platforms. Many organizations look at IT as part of the basis for their competitive edge, whether in terms of the scale, efficiency, capacity, or capabilities their IT environment delivers. In these cases, businesses may do a lot of custom development or adopt more specialized, niche types of products. Examples of these types of approaches abound:

- A utility may need a way to remotely monitor "smart" meters deployed at customer sites.
- A business may opt to use a power management tool that is specific to a type of server racking system that is used to support the virtualized environment.
- An organization may develop a custom application that runs on top of an Oracle database, which means the health and performance of the application needs to be monitored and correlated with the performance of the database application.
- A large enterprise may develop their own specific infrastructure management portal to provide on-demand resources within a VMware server farm—and display monitoring data to users in a custom dashboard that features account information and server status.

In these cases, integrating monitoring of the customized or specialized resources, along with the virtualized environment and the broader IT infrastructure, can be a critical endeavor. Toward that end, businesses need to employ monitoring solutions that offer integration flexibility, for example, through both standard APIs and the ability to develop custom data collectors.

may want to have monitoring configurations assigned using the CMDB and provisioning system or within VM golden images.

- Identity and access controls. If a business is using Microsoft Active Directory for managing user identities and permissions, they may want to ensure monitoring is effectively integrated with this environment. For example, only a specific group of system administrators might be authorized to access monitoring data from the Oracle Financials applications.
- Lifecycle management tools. An organization may want to apply lifecycle management tools to their virtualized environment, so, for example, they could enforce a policy of making a given VM obsolete if it falls below a certain utilization percentage for a certain period of time. If that is the case, monitoring needs to be aware of this policy when it is enforced, so it gracefully decommissions associated monitoring and alerting settings.
- Security environments. Monitoring, and the data generated, need to be integrated with an organization's security policies and environments, including adhering to standards for data transmission.

Best Practice #6: Track and Communicate the Value of IT and Virtualization

Today, it is more vital than ever for IT teams to track, measure, and demonstrate their value. This is true for two key reasons:

- First, from an IT team's standpoint, the automated, on-demand nature of virtualized environments can be both a blessing and curse: While users may perceive the benefits, they may be even further removed from the individuals responsible for maintaining and delivering those solutions. Consequently, they may wonder about IT's contribution, and the importance of the team's roles within the business.
- Second, businesses increasingly need to compare the relative merits of internal and externally hosted IT services, such as virtualized resources in a public cloud. A business executive could easily and quickly find how much a secure, cloud-based server hosting offering would cost each month. To make the best decisions for their businesses, executives need to be able to understand the cost of hosting a comparable type of service or infrastructure internally.

Thus, IT needs to be armed with accurate, timely information about the cost and value of the internal virtualized infrastructure. While VMware has built-in chargeback capabilities, they are very complex to use, and they are not integrated with the monitoring environment or tied to usage of physical systems. Consequently, with these built-in capabilities alone, it will be next to impossible to gain a complete picture of resource usage and cost of given services.

To knowledgeably assess the cost and value of virtualized environments, businesses need to have usage correlated with physical servers, both those outside and inside the virtual environment. Further, organizations need to tie resource usage back to specific groups or applications. These capabilities are essential in accurately understanding the real-world cost of maintaining a virtualized environment for a given application, service, or business unit.

Nimsoft: Optimizing Performance and Efficiency in Virtualized Environments

The Nimsoft Monitoring Solution (NMS) for VMware offers the sophisticated, comprehensive, and efficient monitoring capabilities that enable organizations to ensure the highest level of availability and performance of their virtualized IT infrastructures. NMS offers the capabilities and characteristics that make it practical and efficient to employ best monitoring practices—and fully leverage the performance, agility, and cost benefits of virtualized infrastructures. With NMS, IT teams can...

Gain a centralized, complete picture of the infrastructure. NMS can monitor VMs, ESX hosts, vCenter, and other elements within the

VMware infrastructure. In addition, NMS monitors the applications that run in the virtualized environment and can deliver accurate insights into the performance that end users experience from these virtualized business applications.

Automate monitoring of VMs. NMS offers a range of automation capabilities that make it ideally suited to dynamic, virtualized VMware environments. As a result, businesses can minimize administrative effort, while leveraging sustained and meaningful monitoring information. NMS can automate discovery, agentless monitoring via policy templates, configuration and deployment of agent-based monitoring, and display.

Correlate physical and virtual resources. With NMS, administrators can monitor and manage not only the core virtualization infrastructure, but all the physical systems that the virtualized environment relies upon, including networking equipment and server platforms. NMS can effectively correlate between the ESX host and associated VMs, with the physical layers underlying the ESX host, and with VMs and resident applications.

Maintain awareness with vMotion, HA, and DRS. Through its robust integration with VMware environments, NMS provides capabilities for automatically detecting when vMotion, HA, and DRS add or remove resources from the virtualized environment, and for effectively retaining monitoring continuity, even when IP or MAC addresses of a given service change.

Fully integrate monitoring with the rest of the infrastructure. NMS offers flexible APIs and customization capabilities that enable organizations to maximize integration, across all layers of monitoring, including data, message bus, operations, and presentation layer. With NMS, event and threshold data can be shared through direct integration with SMS, email, service desk, and CMDB applications. In addition, NMS features software development kits (SDKs) in several programming languages—including Perl, C/C++, VB/VB script, .NET, and Lua—that enable efficient development of custom data collectors.

Track and communicate value of IT and virtualization. By offering a cohesive view of monitoring and resource usage, across the entire physical and virtual IT landscape, NMS enables IT teams to accurately track, and report on, the usage, cost, and value of the virtualized infrastructure.

With all these capabilities, NMS gives administrators the cohesive views they need to more quickly identify and address issues—and to more proactively manage their environment so they can better guard against outages and performance degradation.

Conclusion

To effectively monitor and manage their virtualized environments, IT teams need a complete monitoring solution, one that offers a centralized view of all of the physical, virtual, and application layers and one that automates the discovery and deployment of monitoring. By offering the comprehensive infrastructure coverage of the entire physical and virtualized IT infrastructure—and the intelligence and automation required to efficiently gather and present this monitoring information—NMS delivers the capabilities IT teams need to employ best monitoring practices and realize optimal performance, availability, and value from their IT infrastructures.

Nimsoft Whitepaper

About Nimsoft

Nimsoft is a global leader in IT Management-as-a-Service. The company's lightweight ITMaaS solutions make it easy for enterprises and service providers to implement comprehensive, adaptable monitoring and service desk capabilities essential for managing today's dynamic computing environments. Learn more at www.nimsoft.com.

North America Headquarters
U.S. toll free:
1 877 SLA MGMT (752 6468) 1 408 796 3400

Email: info@nimsoft.com
Web: www.nimsoft.com

United Kingdom
+44 (0) 845 456 7091

Norway & Northern Europe
+47 22 62 71 60

Germany
+49 (0)89 – 99 61 90 60

Australia
+61 (0)2 9236 7216

Brazil
+5511 5503 6243

Mexico City
+52 (55) 5387 5406

Singapore
+65 64328600

New Delhi
+(91 11) 6656 6667

Mumbai
+(91 22) 66413800