



Managing VMware® Doesn't End with Managing VMware

Contents

Why VMware?.....	1
The Changing Management Paradigm	1
Business drivers	2
NetIQ's Approach to Operational VMware Management.....	3
Conclusion.....	5
About NetIQ Corporation	6

White Paper

April 2008

In today's data center, VMware has become a household name. The business benefits of deploying VMware range from saving time, reducing energy consumption, and improving disaster recovery capabilities. Like any technology in the data center, VMware must be managed.

VMware has garnered the lion's share of the server virtualization market in part because VMware, Inc. provides very good management tools for VMware. For many VMware administrators, the VMware tools such as VirtualCenter are up to the task of managing VMware.

For IT operations, the story is much different. Managing VMware is only part of the story. Instead, VMware introduces a new paradigm that alters the very way that IT operations has managed their infrastructures and applications. In doing so, it has become apparent that the old approaches to systems management are not up to the task.

This paper discusses the challenges introduced to systems management as the result of VMware. In addition, it describes NetIQ's approach to Operational VMware Management, an approach that addresses the hybrid physical / virtual environment.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 1995-2007 NetIQ Corporation, all rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAgent, ActiveAnalytics, ActiveAudit, ActiveReporting, ADcheck, Aegis, AppAnalyzer, AppManager, the cube logo design, Change Administrator, Change Guardian, Compliance Suite, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowing is Everything, Knowledge Scripts, Mission Critical Software for E-Business, MP3check, NetConnect, NetIQ, the NetIQ logo, the NetIQ Partner Network design, Patch Manager, PSAudit, PSDetect, PSPasswordManager, PSSecure, Risk and Compliance Center, Secure Configuration Manager, Security Administration Suite, Security Analyzer, Security Manager, Server Consolidator, VigilEnt, Vivinet, Vulnerability Manager, Work Smarter, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Why VMware?

Virtualization offers numerous business benefits for the enterprise datacenter, such as:

- ❑ **Cost Savings** — the cost savings extend to numerous areas including hardware, software licensing, facilities and real estate. With a recession on the horizon, cost savings will drive increased adoption of VMware in the production environment.
- ❑ **Server Consolidation and Resource Utilization** — quickly optimize the datacenter infrastructure, deploying fewer systems and maximizing server hardware capabilities
- ❑ **Flexible Systems Management** — as the demands peak for various applications during the course of a normal business day or a seasonal period, VMware provides the operational flexibility so that the application can access the maximum resources needed to maintain application availability and performance
- ❑ **Business continuity and disaster recovery** — backup and recovery are key parts of IT strategy and VMware eases the implementation as well as ensuring the greatest uptime and system availability in the event of an outage
- ❑ **Going Green** — operating fewer servers in a datacenter results in energy conservation, less hardware waste when systems are retired and less real estate development for extensive datacenters required all resulting in a positive environmental impact

As a result, VMware is no longer deployed only for test and development environments. Instead, VMware's flagship hypervisor technology, ESX Server, is being deployed in production environments and, over time, to host more and more critical applications. As a result, VMware ESX Server is quickly become part of the mission critical environment.

The Changing Management Paradigm

VMware changes the systems management paradigm. Most importantly, the virtual model means that systems management approaches – and tools – can no longer assume a static environment or one tied to physical hardware. More specifically, there are challenges related to migration, monitoring and security:

Migration

In early phases of VMware deployments, identifying candidates for virtualization is often relatively trivial. It begins with very simple applications such as file and print servers, back-office applications and web servers. Determining candidacy typically means simply evaluating four standard performance indicators of the servers: CPU utilization, memory utilization, disk I/O and network I/O.

Once virtualization of these less critical or less complex applications has been performed, organizations often turn to more complex and demanding applications that may not fit the simple criteria above. Application level metrics become much more important. Without the right tools, successfully identifying and virtualizing these applications lead to long migration planning cycles. Not carefully considering additional metrics beyond the standard four performance indicators will likely result in poor performance of the application once virtualized.

Monitoring

Introducing the hypervisor into the application stack brings new challenges around monitoring hardware, the hypervisor itself, the operating systems and the applications deployed to the virtual machines. Without the system management tools that are optimized for the VMware infrastructure, organizations can lose visibility into the true performance of their applications.

In a virtualized environment, monitoring the performance from an end-user perspective (i.e., end-to-end monitoring) becomes even more important. Oftentimes, users experience poor performance from applications on virtual servers even when server-level performance indicators (e.g., CPU utilization, memory utilization) appear within normal ranges. In other words, the end user experience often differs from the measurements of traditional element monitoring tools.

Maintaining a comprehensive view of both the physical and virtual infrastructure is critical to quickly addressing issues in the IT environment as well correlating metrics for comprehensive reporting for service level agreements.

Security

VMware introduces new security and compliance concerns as well. In particular, the hypervisor represents a new element of risk to the application stack. The VMware ESX hypervisor is currently built on a Linux operating system. As such, the hypervisor must be properly secured (configured, patched, etc.), just as with any layer of technology that supports a critical application.

Another risk inherent to VMware environments is virtual sprawl, or the rapid growth in the number of virtual servers. This often comes with a loose internal control environment whereby virtual servers are not as protected as their physical counterparts. Moreover, security management tools sometimes are not built for the virtual environment and have no visibility into the hypervisor.

Business drivers

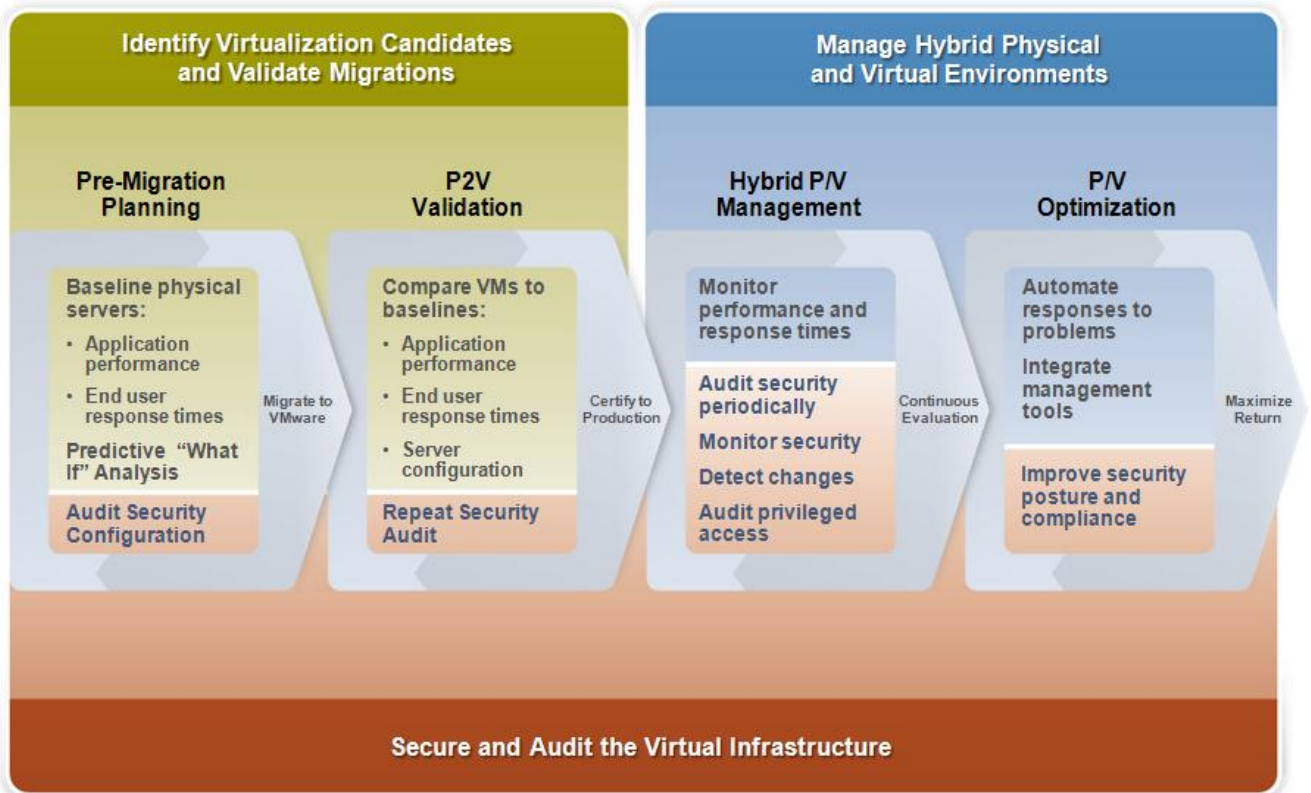
Reducing costs is typically the primary business driver for implementing a VMware strategy. With fewer physical servers, there is a lower hardware maintenance, software licensing, power and cooling and real estate costs. In addition, with reduced number of physical servers, IT staff can be redirected to focus on strategic projects that will further impact the business success.

Although reducing costs is first on the list, it cannot come at the expense of performance and availability of IT services. Management and reporting become more important to track the success of the virtual environment against existing service level agreements and end user expectations. By deploying management tools optimized for both physical and virtual environments, the impact of the more complex virtual infrastructure is reduced to IT operations and applications management teams.

Properly securing corporate data without slowing the progress of IT's virtualization efforts is garnering more attention as the number of virtual machines deployed are increasing. Configuring virtual server hosts consistent with corporate configuration standards is more difficult to monitor and ensure only authorized changes have occurred. In addition, the hypervisor often hides the virtual machines from the view of the security architects leaving systems more vulnerable to attack than their physical counterparts.

NetIQ's Approach to Operational VMware Management

In order to address the challenges of this new management paradigm, NetIQ has developed a systematic approach for operational VMware management, as depicted below. This approach is built upon three main sets of capabilities: identifying virtualization candidates and validating migrations; managing hybrid physical and virtual environments; and securing and auditing the virtual infrastructure.



These capabilities help manage more than just VMware ESX Server; they manage the hybrid physical / virtual stack, including hardware, hypervisor, and virtual machines and applications. Moreover, these three capabilities support a four stage lifecycle for VMware:

- Pre-Migration Planning
- Physical to Virtual Validation
- Hybrid Physical / Virtual Management
- Physical / Virtual Optimization

Each of these stages is described below.

Pre-Migration Planning

Pre-migration planning is critical to ensure a successful migration to the VMware infrastructure. NetIQ AppManager Suite, along with NetIQ Analysis Center, enable IT operations to monitor key performance indicators (KPIs) over an appropriate time period (from days to weeks and months). They can quickly generate reports on the standard four metrics (CPU, memory, disk and network) as well as detailed application performance, historical trending and end user response times. Together, this data provides clear picture of the best candidate for virtualization, pre-migration views of expected server utilization when stacking applications with a single host, and comprehensive baselines or comparison after the application is migrated to the VMware infrastructure.

Another key component of pre-migration planning is performing a security audit on the servers to be virtualized. Server configuration is often modified by the migration process, often introducing service accounts, file shares, new services and network settings. Consequently, it is important to understand the pre-migration security configuration, thereby creating a configuration baseline. NetIQ Secure Configuration Manager audits the security configuration of Windows, Unix, and Linux hosts, along with applications such as databases and web servers. These configuration audits can establish baselines for future (post-migration) comparisons.

Validate Physical-to-Virtual Migration

Once migration is complete, NetIQ recommends monitoring performance (e.g., server and application KPIs) and end user response time, and running reports to ensure consistency of service to pre-migration service levels. With NetIQ AppManager Suite, IT no longer has to wait for the helpdesk phone to ring, but can proactively address performance issues reducing any performance degradation impact to end users.

With the new infrastructure, it is paramount to monitor the VMware infrastructure – specifically ESX Server. Many tools monitor only pieces of the infrastructure, maintain historical data for only short periods of time, or are not scalable to sufficiently meet the needs of an enterprise VMware environment. NetIQ AppManager Suite monitors all aspects of the infrastructure, including the ESX hypervisor, underlying OS, ESX Server host hardware, as well as the virtual machine operating systems and applications.

Finally, it is crucial after migration that the security audit is repeated and that any changes to security configuration are reviewed. NetIQ Secure Configuration Manager audits VMware ESX Server against the Center for Internet Security Benchmark for ESX Server (http://www.cisecurity.org/bench_vm.html).

After monitoring, comparing and assessing performance and security of the virtualized servers, they can be certified for production.

Hybrid Physical / Virtual Management

Ongoing management and monitoring satisfies the next stage of NetIQ's approach. Unfortunately, VMware-specific tools provide a myopic view of system performance. This makes it difficult to identify and resolve many complex issues.

NetIQ AppManager Suite provides comprehensive monitoring and management of the hybrid infrastructure. In addition to having visibility into the entire stack (hardware, hypervisor, VMs and applications), NetIQ's solution correlates events from these different layers, and from end user response time metrics, in order to streamline diagnostics and decrease the time to resolve issues.

NetIQ's report templates for VMware ESX Server quickly provide critical data for capacity planning and optimization of the ESX Servers and resource pools. Together, NetIQ's VMware Management solution is designed to simplify IT performance and availability management for IT operations in an increasingly complex environment.

Physical / Virtual Optimization

The final stage of Operational VMware Management is optimizing the physical and virtual infrastructure. This means two things: optimizing the performance and security of the infrastructure and applications as well as optimizing the management processes. NetIQ's solution provides short- and long-term analytics of performance data, supporting the optimization of the infrastructure itself.

IT process automation helps optimize the VMware management processes. NetIQ supports IT process automation by enabling customers to integrate multi-vendor management tools and automate common tasks, such as problem response. Using NetIQ's IT process automation solution, workflows can be constructed for various tasks commonly performed such as balancing loads between resource pools.

Conclusion

It is clear that there is much more to managing VMware than just managing VMware itself. Data provided through Virtual Center only touches the tip of the iceberg when it comes to ensuring the performance and end user experience of a virtualized application. With service level agreements a critical part of IT's report card, being armed with the data necessary to proactively manage the hybrid virtual and physical datacenter will become a key requirement.

As VMware environments continue to grow, and more complex applications are virtualized, visibility into the virtual machines will be more in demand. Correlating data, quickly diagnosing issues and reducing the mean time to resolve (MTTR) will contribute directly to the success of the VMware deployment and support a faster return on an organization's virtual investment – bringing the lifecycle full circle back to the primary business drive for deploying VMware – costs savings.

About NetIQ Corporation

NetIQ, an Attachmate business, is a leading provider of comprehensive systems and security management solutions that help enterprises maximize IT service delivery and efficiency. With more than 12,000 customers worldwide, NetIQ solutions yield measurable business value and results that dynamic organizations demand. NetIQ's best-of-breed solutions help IT organizations deliver critical business services, mitigate operational risk, and document policy compliance. The company's portfolio of award-winning management solutions includes IT Process Automation, Systems Management, Security Management, Configuration Control and Change Administration.

For more information, please visit <http://www.netiq.com>.