WHITE PAPER

Streamlining Patch Testing and Deployment

Using VMware GSX Server™ with LANDesk® Management Suite to improve patch deployment speed and reliability

LANDesk® SOFTWARE

vmware®

Streamlining Patch Testing and Deployment

Using VMware GSX Server with LANDesk Management Suite to improve patch deployment speed and reliability

Executive Summary

As corporate IT departments work to keep up with the increasing number of threats, vulnerabilities and patches, they are faced with two key challenges—testing patches for compatibility with standard corporate hardware, OS and application configurations, and efficiently deploying critical patches throughout the enterprise.

LANDesk Software and VMware provide solutions for both of these problems. VMware® GSX Server™ enables the creation of virtual machines that run as applications on a single server. That gives IT staff the tools to create and run a variety of standardized test configurations with less cost, faster roll back and reduced management. LANDesk® Management Suite with LANDesk® Patch Manager automates the patch download, distribution and verification process. Used together, these solutions enable fast, efficient patch evaluation, testing and deployment across the enterprise.

Table of Contents

Why configuration testing is so important

While vendor patches are designed to repair vulnerabilities and improve overall system performance and security, it's an unfortunate fact that those patches often create as many problems as they solve. The complex interactions among the wide variety of hardware, OS and application configurations deployed in modern enterprises create unexpected problems and expose previously hidden issues. Ideally, every patch is tested against each major configuration in a lab environment prior to deployment. That way IT can isolate and address problems under controlled conditions before placing their operating environment at risk.

In practice, though, most enterprises have neither the money to set up a dedicated test lab, the time to stage and restore disk images across the large number of test configurations required for exhaustive testing, nor the personnel to thoroughly test each and every patch. According to an article in Network Computing magazine[1], 44% of respondents surveyed identified patch testing as their greatest challenge in the patch deployment process. As a result, many companies either deploy critical patches with little or no testing, or choose not to deploy patches at all until a major security threat requires it—then they push it out as fast as possible and wait for the inevitable compatibility problems and system failures that follow.

Power of virtual test environments

VMware virtual machine software enables the creation of complex test environments with minimumal cost, time and effort. With VMware GSX Server, an unlimited number of virtual machines can be stored on a server and up to 64 can be run simultaneously. Each virtual machine can run a selected operating system configured for specific hardware and running selected applications. VMware enables replication of complex operating environments, including virtual hardware devices such as network adapters, IDE and SCSI disks, USB and so on. Because the complete configuration of a virtual machine is stored in a simple set of files, those disk files can be copied and moved around to facilitate optimal testing and customization.

Running these test configurations on a virtual machine reduces the testing lifecycle time and nearly eliminates delays caused by software corruption or failure—simply discard changes to the virtual machine and return it to the last known good state saved in the disk file. The process takes seconds to complete and enables immediate retesting, rather than waiting hours to reconfigure a physical machine or restore a stored disk image over the network. Because virtual machines are isolated from each other and from their host server, a failure in one virtual machine won't take down your entire testing environment.

This flexibility enables more robust testing across a wider variety of configurations in less time, with fewer resources and less money. Better patch testing leads to greater security and reliability for enterprise computing environments.

VMware GSX Server—perfect for patch test operations

VMware GSX Server allows virtual machine servers to be remotely managed, automatically provisioned, and standardized on a secure, uniform platform. VMware GSX Server has these features critical for hosting test clients:

- GSX Server installs on Windows or Linux hosts for maximum flexibility.
- The Windows or Linux host operating system provides GSX Server and its virtual machines with support for any connected devices – disk storage, networks, SCSI, USB, serial, parallel, etc.
- GSX Server supports the broadest array of Microsoft, Linux and Novell operating systems in its virtual machines.
- GSX Server virtual machines are hardware-independent so they can run without changes on different host servers.
- GSX Server virtual machines can run headless with no need for a connected console that requires resources and can reduce reliability.
- Multiple virtual machines can be powered on and execute tests concurrently.
- Testers can manage and monitor GSX Server virtual machines remotely over any network connection using its web-based management interface and virtual machine console client.
- The GSX Server Scripting API supports remote or programmatic control of virtual machines.

Using VMware with LANDesk Patch Manager

LANDesk Management Suite combines with LANDesk Patch Manager to automate patch research, download, deployment, verification and ongoing maintenance. VMware GSX Server speeds patch testing, conflict discovery and problem resolution. Together, they represent a robust system for quickly and efficiently managing patch deployment throughout the enterprise.

The patch management process consists of these major steps:

- Scan clients to identify vulnerabilities to known problems
- Download the patches needed to remediate detected vulnerabilities
- (Optional) Create a library of standard configurations for testing
- Test patches against target hardware, software and OS configurations and resolve any conflicts or incompatibilities
- (Optional) Create custom patch packages optimized for your environment
- Deploy packages across the enterprise using efficient distribution techniques
- Verify patch deployment with real-time task monitoring and reporting
- Automated ongoing maintenance with application policies

Step 1: Scan for known vulnerabilities

LANDesk Patch Manager automates access to a multiple of information sources to enable complete vulnerability scanning across a wide variety of platforms, applications and languages. Configure recurring vulnerability database updates from the LANDesk patch management datacenter and recurring vulnerability scans on managed clients to detect vulnerabilities using the latest data.

Step 2: Download needed patches

LANDesk Patch Manager makes it easier to sort vulnerable machines, research patch requirements and interactions, and prioritize patch selection, then download selected patches to the local network. Staged patches are now locally available for testing and deployment.

Step 3: (optional) Create a library of standard configurations for testing

With VMware software, a virtual machine including hardware, BIOS, OS, and application configurations, or even a complete network of virtual machines can be stored as a few files.

Stored virtual machines do not consume any computing resources.

This enables you to create pre-configured libraries of standard configurations. When LANDesk Patch Managers identifies a vulnerability that needs to be patched, the relevant test bank of virtual machines is activated for testing. This approach saves you configuration time and enables consistent and exhaustive testing.

Step 4: Test patches against standard configurations

Using virtual machines running on VMware GSX Server, with or without a pre-configured test bank library, you can perform rigorous testing against selected hardware and software configurations, through both manual testing and test automation tools provided in each virtual machine. Exhaustive testing enables you to quickly isolate and resolve problems. Because VMware virtual machines can run LANDesk client agents, you can even test the deployment process itself using LANDesk Management Suite so you can refine deployment scripts and test client restart requirements to increase patch success.

Step 5: (Optional) Create custom patch packages

LANDesk Management Suite features a powerful package builder that includes the ability to use snapshot technology to capture the changes made to a computer's configuration during the patch process. Run the LANDesk Package Builder on a VMware virtual machine to capture the unique requirements needed to successfully deploy a patch to a problematic configuration, or to roll up multiple patches into a single distribution package. Use VMware features to instantly revert virtual machines to their unpatched state for further testing.

Step 6: Deploy patches across the network

LANDesk Management Suite features a powerful software deployment engine that uses exclusive LANDesk® Targeted Multicast™ and LANDesk® Peer Download™ technologies to quickly deploy patches across the enterprise using a minimum of network bandwidth—without dedicated hardware infrastructure on the subnet. Test deployments and scripts by deploying first to VMware virtual machines to work out any problems, then deploy quickly across the enterprise.

Step 7: Verify deployment
LANDesk Management Suite features real-time task monitoring and reporting so you can quickly identify deployment failures. Remote problem resolution tools help IT staff quickly identify and resolve problems. Capture unique configuration issues to a new VMware virtual machine to further refine future patch deployment testing.

Step 8: Automate ongoing patch maintenance
LANDesk Management Suite features extensive application policy management features that enable you to develop policies that automatically bring computers up to standard as new machines are added to the environment or as existing machines are restored from backup image.

Streamlined patch testing and deployment

By using LANDesk Patch Manager in conjunction with VMware GSX Server, IT staff can address the key challenges associated with enterprise patch management—effective patch testing and efficient patch deployment and verification.

The primary benefit is that better patch testing means you discover and repair potential patch incompatibilities or problems before you deploy to the production environment. That means fewer surprises, less downtime and less exposure from unpatched systems.

Additional benefits include:

- Faster, more thorough patch testing with fewer resource requirements
- Substantially reduced hardware requirements for comprehensive environment testing
- No hardware provisioning required—virtual machines can all run on a single GSX Server
- Patches can be tested on multiple configurations concurrently
- Instant roll back of the virtual machine speeds testing and problem resolution
- Specialized and critical configurations can be thoroughly tested to reduce potential for downtime
- Automated custom or rollup patch creation
- Deployment testing in addition to patch testing
- Instant rollback of virtual test machines for further testing

For more information

Contact LANDesk Software at
1-800-982-2130 for more information, or visit our Web site at www.landesk.com for more details on LANDesk Management Suite and LANDesk Patch Manager.

Contact VMware on the Web at
www.vmware.com, send email to sales@vmware.com, or call 877-4VMWARE for more information on VMware GSX Server.

[1] "Patchwork Protection" by Tony Arendt. Network Computing magazine; April 1, 2004; pages 45-54.

VMware, Inc. 3145 Porter Drive Palo Alto CA 94304 USA Tel 650-475-5000 Fax 650-475-5001 www.vmware.com

vmware®