# Global Information Assurance Certification Paper

Author's Name: Dan Horsefield

Date of Submission: 2/15/2004

Descriptive Title: Migrating a Web Application to a More Secure O/S While Enhancing Business Continuity & Scalability

# Migrating a Web Application to a More Secure O/S While Enhancing Business Continuity & Scalability

## Abstract:

This document will explore a real-life case study regarding research and implementation of a solution to problematic concerns with a web server. The concerns include:

A. The overall security of a server on the internal network
B. Business continuity in terms of failover and recovery in the event of a failure
C. Web application performance
D. Overall Cost and Return on Investment
E. The time to implement a solution

The web application interface is a corporate web site used by approximately 50 internal users (a business Intranet).

The solutions found to these problems permitted the developer/administrator of the web site to significantly improve the security of the web application, improve the reliability of the web application in terms of business continuity and reduce the recovery time needed in case of a hardware or software failure.

The overall long-term costs of owning and administering redundant servers for each web application was reduced. The solution also permitted the administrator to reduce the costs associated with licensing the web server while improving the performance and scalability of the web application.

The overall solution involved migrating a Windows 2000 Intranet web application from a standalone server to a Windows 2003[1] Web Edition O/S residing on a Unix-style VMware ESX Server platform on Intel architecture.

## Background:

With numerous Windows vulnerabilities inspiring security patches in 2002, the need for a better way to manage “patching” servers became evident since the company (we will refer to our company as ACME Services) was applying security updates[2] from Microsoft

[1] Microsoft Windows Server System "Upgrading to Windows Server 2003" 2004, URL:http://www.microsoft.com/windowsserver2003/upgrading/default.mspx(15 Feb., 2004)

[2] Microsoft TechNet "Patch Management, Security Updates, and Downloads" 2004, URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/patch/Default.asp (15 Feb., 2004)

at nearly every bi-weekly “maintenance window”. Since potential rollbacks would be time consuming and the one-hour maintenance windows were not sufficient for such potential corrective measures, ACME’s Computer Security Officer could easily measure a significant increase in risk in terms of both business continuity and security risk.

According to the Computer Security Institute, a survey in 2002 confirmed that the threat from computer crime and other information security breaches was continuing unabated and that the costs to business were growing.[3]

ACME had already experienced the need for “patch rollbacks” on it’s Exchange Server and SQL Server systems due to clustering issues with one of the W2K patches in 2002 and a DCOM issue with SQL Server which also was attributed to a patch. The clusters being utilized lost their value because of the inability to quickly resolve the issues and this was a substantial loss of capital expenditures.

ACME’s growth was also causing problems in terms of rack space and expense in the data center. Each time a new major application was placed in production, a primary server and a secondary redundant server were placed in the racks. The secondary server would not be updated, the production system would be patched and then if a “rollback” was necessary ACME would disable the primary (patched) system and enable the “backup” server. The need for more efficient use of the hardware was evident. Initially, the secondary servers had been purchased for load balancing to provide scalability, but the patch management had turned some of the critical secondary servers into dead weight. Scalability had been compromised. Patches were also being postponed.

A number of desktop systems on a makeshift server rack (ACME IT workers referred to it as the company’s “ghetto rack”) needed to be eliminated to bolster reliability, increase space, and reduce power consumption from ACME’s uninterruptible power supply.

Performance and scalability of the servers were other issues made obvious at the time of the annual review of ACME’s Intranet web application and IT infrastructure. ACME’s IT team was building their fist .NET applications and they wanted these new applications to co-exist with existing applications on the W2K servers. The new Windows 2003 operating system held the promise of performance enhancements and compatibility with the new .NET services, but ACME couldn’t easily afford to go buy a lot of new Windows licenses to improve the performance.

## Research:

The IT team knew there were limited funds for improvements and IT “work time” was currently at a premium. ACME couldn’t select a solution that would take a lot of IT time to implement and this somewhat limited their choices.

[3] CSI, “Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row” April 7, 2002 URL: http://www.gocsi.com/press/20020407.jhtml?_requestid=217450 (15 Feb., 2004)

Some IT users at ACME including this author had already experimented with the workstation version of VMWare. The software would permit an entire Windows O/S to co-exist on a desktop without ruining the performance of the main desktop O/S. This doesn't seem significant until you learn that you never have to burn down your O/S again.

The main desktop operating system for the evaluation was W2K when ACME began with a new VMWare shell. This desktop was replaced with a new desktop running WindowsXP. The VMWare shell was moved onto the new desktop with no problems.

All software originally used by the user had been applied to the VMWare "shell" and then the "image" (file) created by VMWare which houses the entire server in the shell could be copied to any other box. This means the entire server could run on just about any other box in ACME's entire operation. ACME just copied a file to the new XP box and turned on the VMWare shell and everything worked, but it worked faster because it capitalized on the enhancements avialble in the new hardware.

This permits IT users to eliminate the need to rebuild their OS if their desktop machine is upgraded or a new laptop is purchased. All their old applications still work and they don't have to reinstall anything. The programmers could put all their programming installations on the shell and move that shell to any other Windows platform where they could take advantage of the new faster hardware/software combination. This portability feature led to further investigation into the feasibility of housing mission critical servers on VMWare.

ACME's network administrator researched the scalability of the data center and took a closer look at an evaluation copy of the VMWare ESX server. Windows tools like WinSCP were readily available at little or no cost to securely manage moving files from the drives on the the Linux-style platform used by VMWare. A 20-minute training session was needed to teach IT workers how to use the VMWare services. This author, acting in the role of Director of Computer Operations, attended a free webcast which outlined the cost savings and ease of migration regarding a move to ESX server and submitted findings from that webcast to management.

We quickly learned that the proverbial learning curve necessary to make VMWare ESX server the answer to our problems was relatively short. We decided that one brief training session of about 30 minutes and little hands-on experience with the network administrator when using the server for the first few times would be all that would be necessary to get ACME's targeted systems including the Intranet application and some "ghetto rack" servers onto the new platform.

## Decision

ACME's IT capital expenditures were reconfigured at management's request to buy two new main servers to house the new ESX server software rather than buy numerous smaller servers. The advantages were clear. We could make more servers with less hardware using the virtual machines. The servers were acquired with about half of their

potential memory and processors capacity. Even at this stripped down state, they could easily support hosting about 8 to 10 virtual machines that were typical for ACME's business.

ACME's Computer Security Officer evaluated Windows 2003 in a development environment and the network administrator also explored the new server. A series of questions regarding capabilities needed for the Intranet application components was posed. It was quickly determined that the low cost Windows 2003 Web Edition would be appropriate since the other services offered by Windows 2003 server were not needed for that specific server.

The security features of Windows 2003 Server were the real deciding factor in selecting this O/S. A Microsoft guide which helped make the decision (dated Dec. 9, 2003) gives an overview of the advantages of security innovations in Windows 2003.

One of the most critical parts of the document explains that Windows 2003 utilizes IIS 6.0 and compartmentalizes the worker processes:

> Third-party application code runs in isolated worker processes, which by default use the new lower-privileged Network Service logon account. Worker process isolation makes it possible to confine a Web site or application to its root directory through Access Control Lists (ACL).[4]

The document, "SecInnovation.doc" can be downloaded from the web page at http://www.microsoft.com/windowsserver2003/techinfo/overview/secinnovation.mspx

## Advantages of VMWare[5]:

Some of the advantages of VMWare explored became useful when we acquired the new servers:

Scalability: Enterprises like ACME could run all their mission-critical applications in flexible, secure, and portable virtual machines. When the server housing the virtual machines is "enhanced" with more memory, drive space, etc. all the virtual machines can be easily configured to take advantage of the hardware improvements.

High Availability: VMware ESX Server allows clustering of virtual machines inside the same system for development and test purposes, or between systems for high availability. It guarantees server resources for CPU, memory, network bandwidth, and disk I/O at optimum performance levels, improving service to internal and external customers of ACME

---

[4] Microsoft Corporation, "Windows Server 2003 Security", March, 2003, available from link at URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/secinnovation.mspx (15 Feb., 2004)

[5] VMWare, Inc. "Server Products -- VMware ESX Server 2 -- Features." 2004, URL: http://www.vmware.com/products/server/esx_features.html (15 Feb, 2004)

Portability: VMware ESX Server encapsulates virtual machine images so that they can easily be moved from environment to environment enhancing the ability to failover to a secondary server by simply attaching to the same virtual machine image (file) used by the primary server. This could be done from a SAN (Storage Area Network device used for production) or from local hard drive files (snapshot backup copies of the server image).

Server Consolidation: VMware ESX Server consolidates applications and infrastructure services running on diverse operating systems onto fewer highly scalable, reliable enterprise-class servers, including blade servers.

Not among the main features cited above (see footnote regarding features of VMWare) was a less obvious feature discovered during evaluation of the software. The ability to use "undoable mode"[6] on each virtual machine provided a significant benefit. This mode provided the ability to patch a system and rollback immediately and completely (on any O/S running on a Virtual Machine) with no significant effort. Patch management had been identified as a major concern for everyone at ACME who had ever participated in security or computer administration training.

## Plan the Move:

Writing and maintaining technical procedures for deploying any application is an important part of business continuity planning. The backup and recovery plan requires access to such documentation. Updating the existing procedures was a good place to to begin planning for the migration. In the case of ACME's web application, a number of functional additions and modifications had been made and documented, but the overall procedures for deploying those programs and functionality had not been updated. Such things to include in the document are specific users, user permissions required, user passwords, what identity certain COM+ components run under, etc.

A checklist itemizing all the subcomponents, names of web page directories, special directory permissions, local users needed, etc. was developed.

## Migrating the Application:

Moving the bulk of the web application and preliminary testing took the author considerably less than one working day.

Testing for functionality, performance and security vulnerabilities caused a significant delay in implementing the changeover. The need for making some unrelated decisions also delayed moving the new web site into production for more than a week. The reasons for the delay included skepticism about the reliability of the new

[6] VMWare Support "Disk Modes: Persistent, Undoable and Nonpersistent" 2004, URL:http://www.vmware.com/support/gsx25/doc/disks_modes_gsx.html(15 Feb., 2004)

hardware/software platform and the fact that Windows 2003 was a new server platform for ACME. Also there was an issue with mapping software which required the Microsoft Java Virtual Machine, which is not deployed with the new OS. The problem was discovered in troubleshooting (the mapping software failed to load maps) and the resolution was to separately install Microsoft Virtual Machine to get the legacy application to work. Windows Update was used to bring the Microsoft Virtual Machine to the latest patch revision.

A recent web page at Microsoft may provide some assistance if you have a similar problem - "Transitioning from the Microsoft Java Virtual Machine"[7].

A brief training course was held to show users how to use the easy VMWare Web interface to "create" a new virtual machine. Training included teaching the ability to attach to a CDROM image containing the Windows server software and quickly install the Windows 2003 Web Edition server on the virtual machine. Users were taught how to toggle back and forth from undoable mode to persistent mode to apply patches. This is done at the server's "reboot" time. You shut down the server and if you are using an undoable disk mode you are prompted to commit or discard the changes. You reselect the mode in the VMWare interface and then start the server. The user can start with undoable mode and change to persistent mode to accept or "commit" all changes after you test the server following application of a patch or revision.

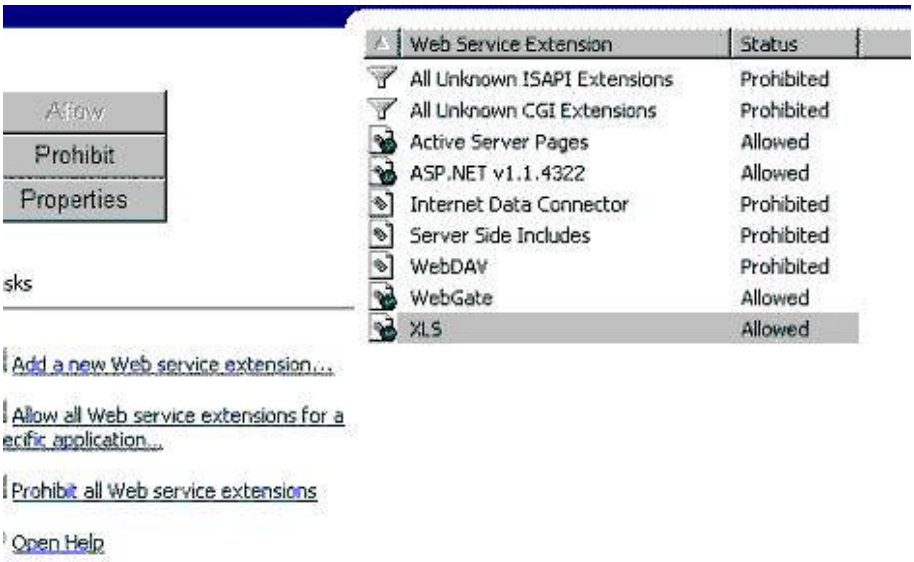
We installed Windows 2003 Web Edition quickly on a new virtual machine shell. The Computer Security Officer followed up with vulnerability scanning. The rest was pretty much a procedure that had been followed when creating the redundant servers that formerly had to be maintained in the event of failures.

A. The main web files (ASP pages, include files, scripts, COM+ files, etc.) were copied to a directory structure on the new web server that was very similar to the existing production server. In IIS manager turn off the default and administration web sites. Right click on the web sites icon and select new, web site. Right click your new web site, select properties and insert the temporary IP address your server will answer requests on (later you will change this to the production IP address when you are ready to implement the switch form the old server). Now type in your directory path to the new web application pages.
B. Deploy scripts should be executed to install the COM+ components and/or related services. The files used by these components will reside on the web server lower in the directory structure than the C:\inetpub\wwwroot directory and only administrators of the web application and the local system account should be allowed to access this location. NOTE: You aren't going see a directory C:\WINNT so make sure the deploy scripts are modified to refer to C:\Windows on Windows 2003. The web pages themselves this time resided on a SAN

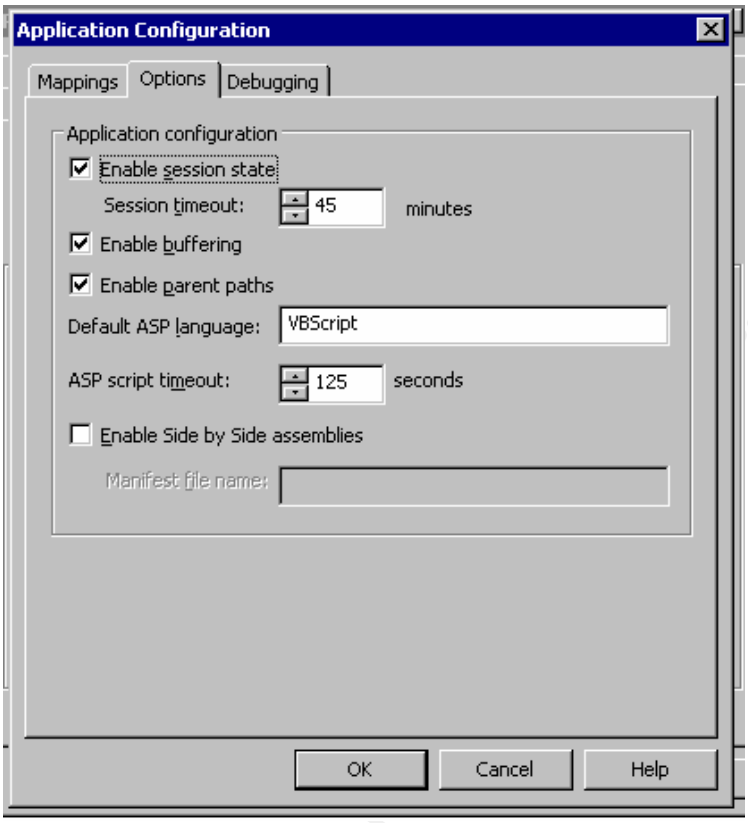
[7] Microsoft Corporation "Transitioning from the Microsoft Java Virtual Machine", Oct. 7, 2003 URL: http://www.microsoft.com/mscorp/java/ (15 Feb, 2004)

whereas they had previously resided on a local hard drive. Some of the files were *.dlls that we needed to register manually or through command-line scripts.

C. Configuring the web extensions was very simple. By opening the IIS manager and selecting the Web Extensions button, you can see that hardly any extensions are “allowed” by default. Here you can add an extension. We added the WebGate extension to support a mapping application that was part of our Intranet.




D. Now we use IIS manager to set the session timeouts. Note: If you have a hard-coded session timeout in your asp pages the timeout value in your asp page will be the default. Changes to some include files, in my early experience with Windows 2003, had been known to “bump” active sessions users have on the server, forcing workers to login again. Make “certain” these planned modifications to server-side include files are only made during your maintenance window or apply them after-hours if your web application doesn’t require 24 hours of availability. Also, when you change user permissions on Windows 2003 you will also interfere with active web sessions. While on this page make certain you have checked the checkbox entitled “Enable buffering”. If you don’t enable buffering, your performance will be slow when the web application attempts to stream HTML before it has been compiled on the server.




E. Use IIS manager to view the ISAPI extensions. By default in Win 2003 Web Edition there will be ASP extensions, numerous .NET framework extensions, but you will not see .hta and .htr extensions which had been targets to security vulnerabilities in the past. If you see these or other extensions that your application does not use, research them to make sure you don't need them, then eliminate them.
F. Make sure you configure your special file/directory permissions on the web server. There are two directories in ACME's Intranet web application that hold reports from external applications. One external application is Active Data Reports which is used to generate files in *.PDF format. The other application is Microsoft Excel which generates files in *.csv and *.xls format. These directories that contain the reports need special "write" permissions configured to allow the web application to have access to the hard drive. You can do this through the Windows Explorer window or the IIS Manager.
G. There's no way we can cover every possible setting you will want to configure on your web server, but the intent here is to remind you there are steps you don't want to forget and which will illustrate that configuring your web server in Windows 2003 is fairly straight-forward with few surprises.
H. Make sure if you have third-party applications, that you use the installation programs provided with the applications to install those. We used RouteMap and Active Data Reports installation programs to create functionality for viewing maps and generating and viewing reports from our ASP pages.

After you follow these basic steps and any procedural steps your particular application may require, you will want to turn on your web site and test the functionality of your applications. If you find broken links, make sure you checked the box in IIS Manager entitled “Enable Parent Paths”. Also, you may get some interesting problems associated with user permissions that will take some time to work through. Do not compromise security of the application by elevating the overall privileges of the user that the web application runs under. This is a big “no-no” from a security perspective and generally makes it harder to narrow down the root problem. If your COM+ components impersonate a local user on the box, you will need to make sure such a local user is created on the server and has adequate access to related system objects.

It is helpful to use the “Event Viewer” on the server to discover and troubleshoot these kinds of permission problems. Use the security icon in the Event Viewer and visually scan for “object access” failures.

Now that you have installed the application and turned it on and tested your functionality, you will want to use a vulnerability scanner again to make sure you have the latest patches for your operating system. Also use a port scanning application to determine if there are any unused services opening ports on the system which are not needed.

Our Intranet application allows all users to connect to the web site and then they must login with a username/password combination which matches settings in our database. To make this more difficult to compromise, you may wish to use the initial password to generate a hash and store that hash in the database and then compare the hash from the login to the hash in the database. This will make it more difficult for password guessing and password attacks partly just because of the length of the hash and partly because of the difficulty of having to generate and pass a hash for each possible password.

Try to use past known vulnerability exploits to access files and information on the web server from your web site address bar. All directory traversal attempts failed miserably when we tried those and everything else you would expect to be “patched” in this O/S was working the way it was supposed to.

Run Windows update at every maintenance window and after a significant waiting period if no problems are apparent. If a problem is encountered, then stop the server, do not commit the recent changes (discard changes) and then restart in undoable mode. If you don’t encounter problems, stop the system, commit the changes and place the server in persistent mode. Return to undoable mode prior to any subsequent system patches or rollouts.

Run the IIS Lockdown tool to harden your box if necessary. Do not use the lockdown tool if you are not familiar with using the tool. Practice in a development environment to gain that skill. You may want to investigate with your network administrator whether your organization has an appropriate group policy (domain security policy) for servers of

this nature. Such a policy may be appropriate for managing the security of this server. You may also want to investigate the value of Security Templates if you have resources on the box which are of high asset value to the company and must not be compromised.

In our Intranet application this was not the case, but on a nearly identical server which resides on an Extranet server (accessed from the Internet), we were using all the same files. On the Extranet server we had a connection to a financials database which was of high asset value. On that server we required SSL connections and we secured the box by explicitly granting access to specific IP addresses of our business partners who acted as vendors for us. We also limited some of the functionality of the box using different database connection strings on a few of the critical pages.

When you have completed your plan of execution and you are confident the server is secure and functional, turn off the original Intranet server and let it sit for a few days (remember to always have a backup plan in case something still isn't working up to par).

Now change your IP addresses for your network adapter in your virtual machine O/S and in your IIS Manager so the web application will respond to the IP address formerly used by the server you turned off. Note: If you are using terminal services to work on the new server (faster), use the web interface that comes with VMWare instead of a terminal session so you don't lose connection with the server when the IP address is changed.

Have the network administrator publish a DNS change and flush the DNS cache so users can find your new web server by the DNS name. Advise and assist users in terminating their use of any old bookmarks that may have referred to an obsolete machine name or DNS name on the network (the server you turned off). Now you are all set.

## Managing Your Virtual Server:

The basic management of the Virtual Server requires that you keep a backup copy of your image file that "is your web server O/S" and also make sure the production file image of your server is accessible from another server that can pick it up in the case of a failover. To copy and move files on the VMWare server, the network administrator can provide you with a user account and password and you can utilize WinSCP (available for free from www.download.com) to connect to the server securely and use SFTP to copy files from the source drive to your local drive or other external target drive. You can also copy from the internal drives by creating a secure user session on the VMWare server.

In the migration scenario we built with two identical VMWare servers, we placed half our new virtual machines on each box so that if hardware on either of the servers failed, we could quickly start up the "server image file" of each of the virtual machines that were hosted by the broken server. And in the event that the SAN failed "production copy of

the image is not available" we can use a recent copy of the image (a backup function creates these) from the local hard drive on the working server.

We have planned for growth and intend to add a third VMWare server after enhancing the available processors and memory on the two initial servers. This will introduce a new scenario in which we can use a VMWare virtual console to balance the load between the servers and move the application shells from server to server in real-time using some of the latest technology available on the VMWare platform.

This will require a gigabit network pipe so we have had to make provisions for that before using the third server. This will dramatically increase our overall resources because we can build out as many virtual machines as two complete servers combined can handle. We currently can only build out what one server can handle in terms of capacity in order to have complete failover capability on the two servers.

In addition to managing the VMWare, you may also want to tune for performance. There are two ways. Since we have database procedures being fired from our ASP pages, we can tune SQL server for each stored procedure. This involves a database manager identifying the worse-performing scripts from a test run and selecting those that need to be more efficient and using database tools to identify additional indexes to make the queries more efficient. Another way is to use Microsoft's Tuning and Performance Guide to get the most out of the Windows operating system.

**Summary:**

VMWare offers "undoable" mode which makes Patch Management attempts "completely recoverable" on any Windows O/S (and Linux and other operating systems) by simply shutting down the server, changing a setting (not accepting changes since last startup) and restarting the server. This allows the user to return to the "state of the server" which was in effect prior to applying the patch.

This permits easy patch implementation and testing in development, staging and/or production environments with complete rollback control.

Windows 2003 Web Edition offers a significant licensing cost advantage and has the server capabilities to serve up .NET and ASP pages, legacy HTML pages, and even supports custom-built COM+ components and third-party applications without any significant problems or concerns in migration.

Migration is not difficult even with home-baked VB code modules and C-style COM+ components to deploy. However there is a significant advantage in terms of security and redundancy/failover.

IIS out of the box (default configuration) on Win 2003 Web Edition significantly limits the potential for many known security vulnerabilities by limiting services and web file extensions.

The VMWare platform offers "immediate" failover in the event that a hardware/software problem would render a primary server unavailable. By simply "attaching" to the “image” (file) that represents the entire server, an administrator can be back in business on another box with no "rebuild time" and no "re-deploy time". This reduces the potential for introducing new vulnerabilities because those are often introduced by the former demands of keeping redundant servers "in-sync" or to keep them at equal patch levels.

The VMWare platform expands the administrator’s options in terms of scalability and performance. Hardware expansion can be utilized immediately by all virtual machines (all the individual operating systems) residing on the VMWare server. The maintenance of the system as a whole requires fewer administrator resources.

Internally written VB and C+ code components and third party applications used by the web site can be accommodated with no need for rewrites.

Despite what you may have heard or read about Windows Update causing problems with servers can probably be attributed to people who have had to conduct a rollback after a patch was applied. Remember that VMWare mitigates this potential for disaster and you can update your system without fear at every maintenance window. If something fails, stop the server and restart it without changing the mode and the new patches won’t be applied. Then you can pick and choose what patches to install and then stop the server, change the mode and thus apply those changes. Don’t forget to return the server to undoable mode after “accepting changes”.

You may want to look into new features like the Server Management System and the Software Update Server capabilities which can be used to assist your organization with patch management administration. ACME is currently testing this on desktops and plans to use it on critical systems if it consistently improves overall security on the local network.

References

Microsoft Windows Server System "Upgrading to Windows Server 2003" 2004, URL:http://www.microsoft.com/windowsserver2003/upgrading/default.mspx(15 Feb., 2004)

Microsoft TechNet "Patch Managment, Security Updates, and Downloads" 2004, URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/patch/Default.asp (15 Feb., 2004)

CSI, “Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row” April 7, 2002 URL: http://www.gocsi.com/press/20020407.jhtml?_requestid=217450 (15 Feb., 2004)

Microsoft Corporation, “Windows Server 2003 Security”, March, 2003, available from link at URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/secinnovation.mspx (15 Feb., 2004)

VMWare, Inc. "Server Products -- VMware ESX Server 2 -- Features." 2004, URL: http://www.vmware.com/products/server/esx_features.html (15 Feb, 2004)

VMWare Support "Disk Modes: Persistent, Undoable and Nonpersistent" 2004, URL:http://www.vmware.com/support/gsx25/doc/disks_modes_gsx.html(15 Feb., 2004)

Microsoft Corporation “Transitioning from the Microsoft Java Virtual Machine”, Oct. 7, 2003 URL: http://www.microsoft.com/mscorp/java/ (15 Feb, 2004)

Windows Server System "Security Patch Management Using the SUS Feature Pack" March 18, 2003 URL:http://www.microsoft.com/smserver/evaluation/datasheets/PatchDeploy.aspasp (15 Feb, 2004)