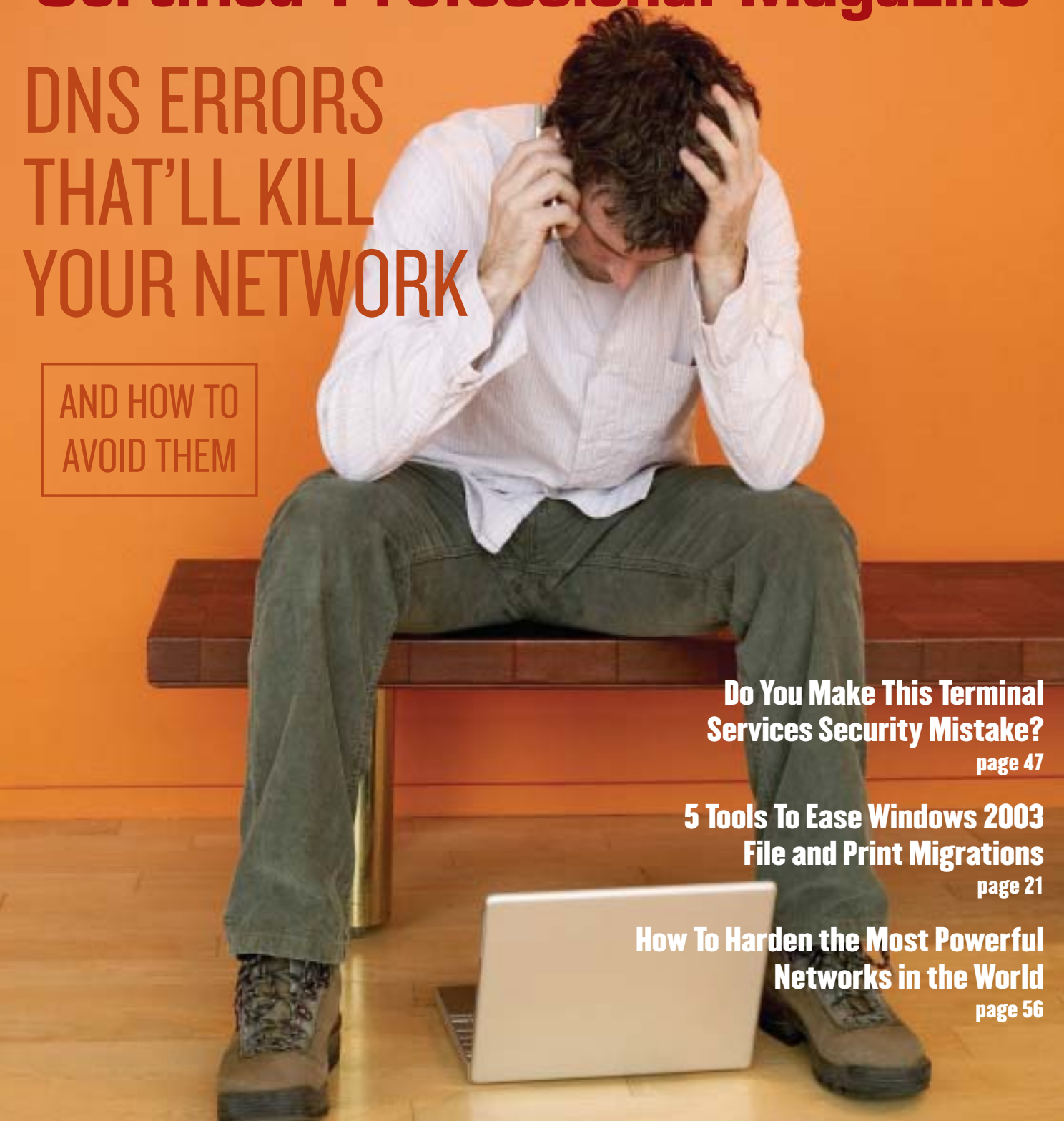
A 101communications Publication

MICROSOFT®
Certified Professional Magazine

DNS ERRORS THAT'LL KILL YOUR NETWORK

AND HOW TO AVOID THEM



Do You Make This Terminal Services Security Mistake?
page 47

5 Tools To Ease Windows 2003 File and Print Migrations
page 21

How To Harden the Most Powerful Networks in the World
page 56

IronPort C60

Powering and Protecting Business Email

BRIGHTMAIL

With Industry leading BRIGHTMAIL™ anti-spam technology.

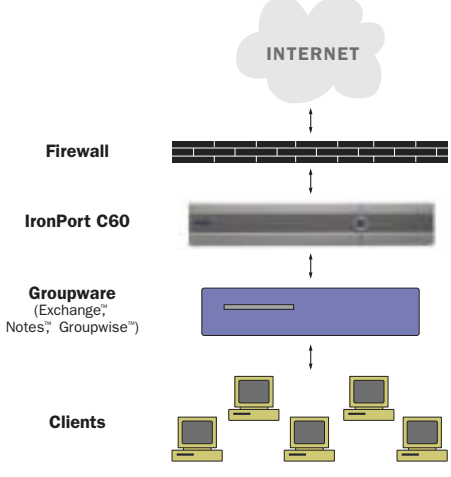
IronPort C60 **Overview**

Overview

The IronPort C60: Powering and Protecting Business Email

The IronPort C60™ Messaging Gateway™ appliance eliminates spam, enforces corporate policy, secures the network perimeter, and reduces the Total Cost of Ownership (TCO) of enterprise email infrastructure.

The appliance deploys between the firewall and groupware servers to power and protect email flowing in from or out to the Internet. Built on the highest performance gateway platform in the world, the IronPort C60 is a multi-function device that provides a single easy-to-use interface for the management of corporate mail flow.



The IronPort C60 integrates easily into existing messaging infrastructures.

FEATURING:

Anti-Spam
The most effective spam control in the industry with two layers of protection. The outer layer is IronPort's unique reputation filter, the inner layer is Brightmail filtering.

Email Access Control
Reputation filters automatically assign policy limits to email senders based on their trustworthiness. Untrustworthy senders have throttled delivery rates.

Mail Flow Monitor™
Automated anomaly detection and complete view of mail flow into or out of the corporate network.

High Performance
The world's fastest gateway, processing more than 500,000 messages per hour.

Corporate Policy Enforcement
Flexible message filter language allows for corporate policy enforcement. Scan message headers, bodies and attachments for keywords.

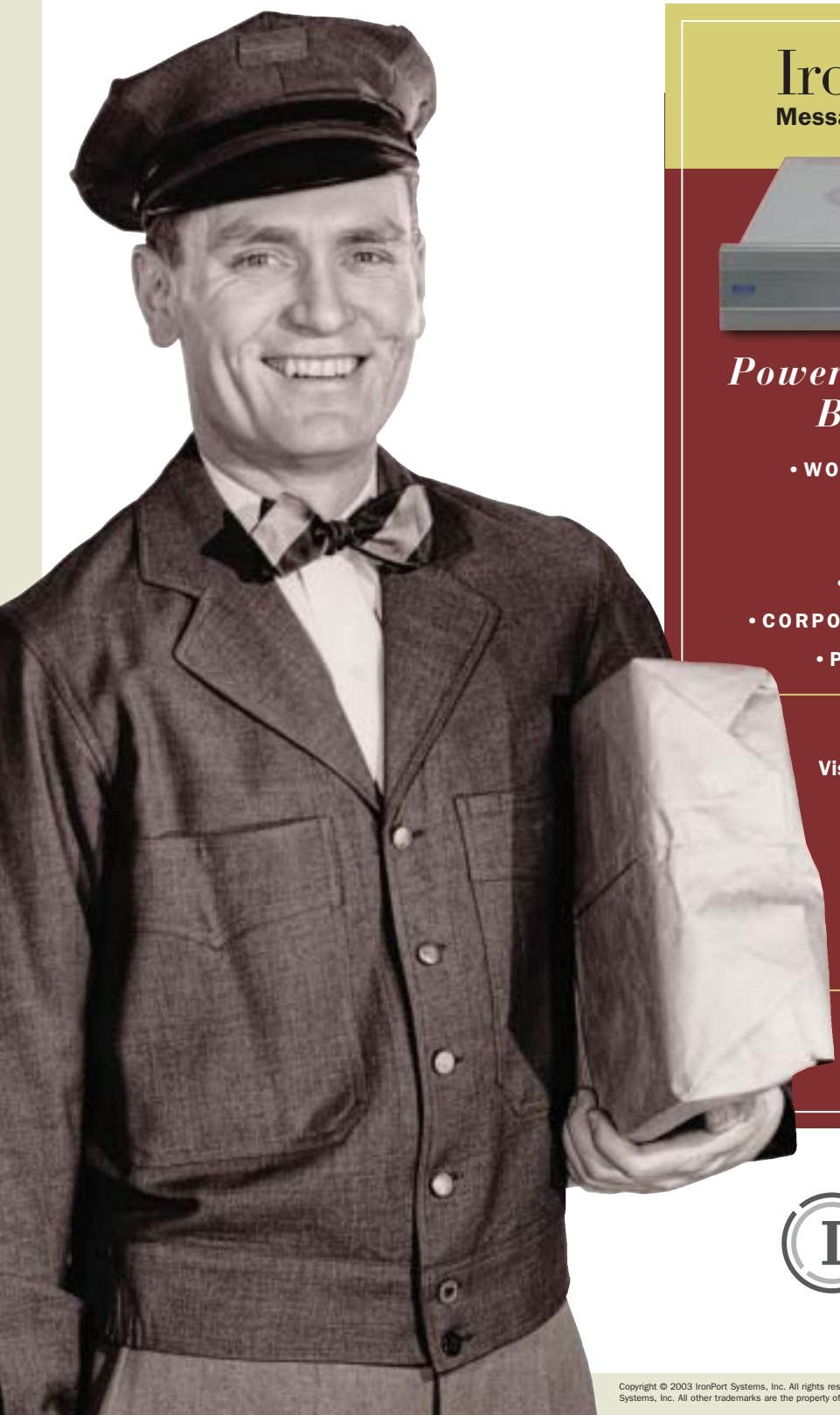
Enterprise Class Solution
Alias tables for message routing, domain masquerading hides internal network details, domain-based routing for hosting multiple domains.

AsyncOS™
IronPort's hardened operating system optimized for messaging. Highly secure with all unused services removed.

IRONPORT™

IronPort Systems, Inc. 1100 Grundy Lane, Suite 100 San Bruno, California 94066 **tel** 650.989.6500 **fax** 650.989.6543 **email** info@ironport.com **web** www.ironport.com

Not your father's MTA.



IronPort C60™

Messaging Gateway™ Appliance

Powering and Protecting Business Email

- WORLD'S FASTEST GATEWAY
- ANTI-SPAM
- ANTI-VIRUS
- MAILFLOW MONITOR
- CORPORATE POLICY ENFORCEMENT
- POWERED BY ASYNCOS™

Learn More

Visit www.ironport.com/webcast

View the IronPort C60 Webcast

FEATURING

Michael Osterman, Analyst
Bailey Szeto, Cisco Systems

email info@ironport.com
phone 650.989.6530
www.ironport.com

IRONPORT™

Stop porn and other harmful content with SurfControl Web Filter

Take back control of your network. SurfControl blocks all forms of unwanted Web content such as porn, gambling and spyware using the industry's most comprehensive, accurate list of categorized URLs. And with remote administration and tailored reporting, you really get the upper hand. No wonder IT professionals voted SurfControl the best Web filter*.

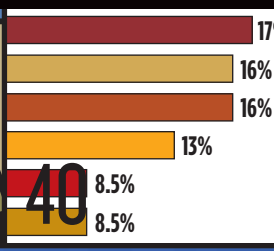
Download SurfControl Web Filter for a free 30-day evaluation now at www.surfcontrol.com or call us at **1 800.368.3366**. *Because network abuse hurts.*

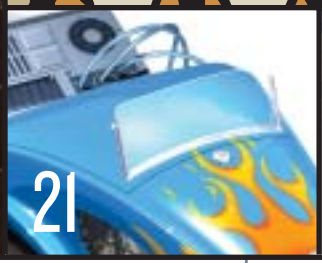
** Winner of the 2003 Microsoft Certified Professional's Best Web Filter award in the "Monitoring Employee Web Usage" category.*

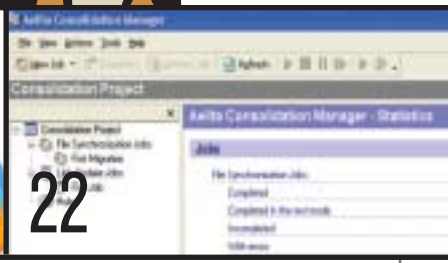
SurfControl®
The World's #1 Web & E-mail Filtering Company

MICROSOFT
Certified Professional Magazine

MAY 2004 VOLUME 10 NUMBER 5
WWW.MCPMAG.COM







COVER STORY

FEATURES

REVIEWS

NEWS

COLUMNS

"THERE WOULD HAVE TO BE MS PRISON FOR PEOPLE LIKE ME WHO CAN'T KEEP THEIR MOUTHS SHUT."

—LOYAL BLAIR
MIAMISBURG, OHIO

MAIL, PAGE 8

ALSO IN THIS ISSUE

Cover Photo by Scott Tysick

MAY ONLINE ARTICLES CAN BE READ AT

MCPMAG.COM/ISSUE/

MCP COMMUNITY

Live Chats
mcpmag.com/chats
Schedule, rules, guidelines and transcripts.

Discussion Forums
mcpmag.com/forums/
Join your peers for technical and certification discussions.

MCP Database
mcpmag.com/mcpdatabase
Join the MCP Database and find fellow titleholders in your region.

MCP TechMentor
techmentorevents.com
Training events for people who manage Windows networks.

MCPmag.com RSS Feeds
mcpmag.com/rss/
Get headline feeds as the news is posted.

FREE E-NEWSLETTERS

MCP Magazine News
lists.101com.com/NLS/pages/main.asp?NL=mcpmag

Security Watch
lists.101com.com/NLS/pages/main.asp?NL=ent&o=security

ENT Newsline
lists.101com.com/NLS/pages/main.asp?NL=ENT

CertCities.com
lists.101com.com/NLS/pages/main.asp?NL=certcities

TCPmag.com
lists.101com.com/NLS/pages/main.asp?NL=tcp

ONLINE THIS MONTH...

REVIEWS

Undelete 4.0
Hit that delete key a bit too early? Executive Software can get that file back.
Reviewed by Danielle and Nelson Ruest

Diskeeper 8.0
This Executive Software tool restores hard drive performance with a thorough defrag.
Reviewed by Mike Morgan

COLUMNS

Solution Developer
Classic (De)Bug
Some things never go out of style, like the advice Steve Maguire dishes out in *Debugging the Development Process*.
By Mike Gunderloy
http://mcpmag.com/columns/developer

Boswell's Q&A
The Island Effect
This reader has trouble with DCs looking within when doing DNS lookups.
By Bill Boswell
More Q&A at http://mcpmag.com/columns/qanda/

Windows Tip Sheet
Seriously, Least Access
Run legacy apps without hitting the security barrier.
By Don Jones
More Tip Sheets at http://mcpmag.com/columns/tipsheet/

EXCHANGE SERVER 2003: REVIEW FROM THE TRENCHES

MCP Magazine readers share their real-world experiences in this no-hype review of Microsoft's enterprise messaging platform.
http://mcpmag.com/resources/exchange_reviewed/

ENTMAG.COM

Network Attached Storage
Special Report: How will NAS shape up now that Microsoft's Storage Server System enters a market book-ended by EMC on the high end and Dell—in partnership with EMC—on the low end?
http://entmag.com/reports/article.asp?EditorialsID=60

CERTCITIES.COM

Security+: What a Disappointment!
Greg Neilson tackles CompTIA's security exam and comes away wishing he'd spent the test fee on expanding his CD collection.
http://certcities.com/editorial/columns/story.asp?EditorialsID=176

TCPMAG.COM

2004 International Salary Survey Online
Cisco technical professionals can only really understand where they stand in the scheme of compensation when they compare their lot to IT professionals in other countries. This year we provide data not only for the U.S., but also for Australia, Canada, Great Britain, India and Singapore.
http://tcpmag.com/salarysurveys/

HEAR IT EXPERTS ON MCPMAG.COM

▶ **Every Friday**	**IT News Roundup**	**Michael Domingo**	**IT News: Listen, Win!**
▶ **April 26**	**MCP Radio**	**Anton Zajac**	**Eset Software's NOD32**
▶ **May 6**	**5 p.m.**	**Andy Barkl**	**70-292, MCSA Upgrade**
▶ **May 13**	**4 p.m.**	**Bill Boswell**	**DNS Errors**
▶ **May 19**	**4 p.m.**	**Andy Goodman**	**Small Business Server Live!**
▶ **May 27**	**5 p.m.**	**Andy Barkl**	**70-296, MCSE Upgrade**

Chat times are based on Pacific (Los Angeles) time zone. Chats are also subject to rescheduling.
For the latest schedule, rules, details and transcripts, go to mcpmag.com/chats.

▶ Live Chat, May 13: Bill Boswell helps you avoid the root causes of the most common DNS errors.

Peer-to-peer is clearly a problem.

Take a close look at the serious security, infrastructure and legal liability threats P2P file sharing poses to your organization. Reduce your risk with Websense Enterprise®. Block access to P2P protocols, sites and applications with the only software that offers end-to-end policy control to effectively eliminate P2P security breaches and other dangers. Stay focused on the P2P solution with a **free white paper** and assess your risks at **www.websense.com/p2p.**

WEBSENSE®

FILTER | PROTECT | OPTIMIZE

DIAN SCHAFFHAUSER

EDITOR'S DESK

What's Your Level?

According to a recent ENTmag.com survey (you can read a summary on page 39), 60 percent of Windows sites already have Windows 2003 in production or plan to do so soon. One major driver is Active Directory. As your job becomes more control-based (via directory services), one would think that meant you had increasing control of your IT operations, too. But it isn't happening like that, according to one of the largest vendors of tools to help you achieve managed data center paradise.

In a recent meeting, NetIQ, which produces AppManager and other products, shared with me a pyramid on management maturity that shows four levels of "IT Responsiveness." At the bottom was "reactive," topped by "managed," then "optimized" and at the zenith, "agile."

David Pann, VP of product management for NetIQ, has been in the software industry for a couple of decades. He started off as a software engineer, then moved into IS and from there management and marketing. He's seen IT from many different angles, and he doesn't find much agility out there. In his experience, 80 percent of companies operate somewhere between the very bottom of "reactive" and the midway point of "managed"—great for his firm's market potential, lousy for you. Reactive companies are characterized by a constant state of unruliness and system outages. Frequently, users (or, more likely, their managers) call the shots on IT decisions. IT staff is underfunded, short-handed and generally overwhelmed by the work at hand.

I decided to do a little poll at the latest MCP TechMentor conference to see if implementers in the trenches agree with Pann about the state of their operations. Sadly, they did. Some cited management or clients who only want to pay (dearly) when something goes wrong, not for maintenance to prevent the problems. Others said budget restrictions prevented them from accomplishing all they could. The only person who said otherwise worked in a healthcare firm in Puerto Rico. He thanked his director for pushing for the resources they needed to put his company between the managed and optimized level. And therein lies a clue to managed nirvana: the champion who can sell.

According to Pann, what IT people still need to do is get better at building the business case. "If you go in and try to sell on features and functionality, it's a hard one... [You have to] be able to go in and say, this is the kind of information we don't have at our disposal today. These are the kinds of decisions we can make. This is the kind of information I can deliver to you on a regular basis." The first step needs to be to talk with your "customers"—clients, users, management—to discover their perception of IT operations. Then you need to figure out how to fix any misalignment that's in place. Interestingly, this product person believes the solution might not be a product; it's just as likely to be better communication or a different process.

Anybody out there at the optimized or agile level? How did you get there? Tell me at dian.schaffhauser@mcpmag.com, and I'll tell others.

MICROSOFT
Certified Professional Magazine

May 2004 Vol. 10 ▪ No. 5

Editorial Director Dian Schaffhauser dian.schaffhauser@mcpmag.com
Senior Editor Keith Ward, MCSE keith.ward@mcpmag.com
Reviews Editor Doug Barney doug.barney@mcpmag.com
Editor, MCPmag.com Michael Domingo michael.domingo@mcpmag.com
Editor, CertCities.com Becky Nagel bnagel@101com.com
Editor, ENTmag.com Scott Bekker sbekker@entmag.com
Associate Editor Kristen Kazarian kristen.kazarian@mcpmag.com

Contributing Editors Bill Boswell, MCSE; Roberta Bragg, MCSE; Harry Brelsford, MCSE, MCT; Chris Brooke, MCSE; Mike Gunderloy, MCSE, MCSD, MCDBA, MCAD; Don Jones, MCSE
Contributing Online Editor Andy Barkl, MCSE, MCT
Contributing Writer Em C. Pea, MCP

Acting Art Director Scott Rovin
Art Director Michele Singh
Graphic Designers Steven L. Anderson; Graye Smith

Publisher Henry Allain
Associate Publisher Matt N. Morollo
Manufacturing & Distribution Director Carlos Gonzalez
Director of Audience Development Phil Tsang
Production Manager Videssa Djucich
Marketing Manager Michele Imgrund
Production Coordinator Niesha Alexander
Senior Web Developer Rita Zurcher
MCP TechMentor Conferences Marketing Director Kay Heitzman
Conference Sales Director Al Tiano
Conference Operations Manager Sara Seely
Conference Marketing Manager Susan Knight
Conference Program Manager Jim Turner

101communications
Enabling Technology Professionals to Succeed

President & CEO Jeffrey S. Klein
Executive VP Steven Crofts
Executive VP Gordon Haight
Senior VP & CFO Stuart K. Coppens
Senior VP, CIO & General Counsel Sheryl L. Katz
Senior VP, Operations Bradford C. Stauffer
Senior VP, Human Resources Michael J. Valenti

MCPmag.com

Postmaster: Send address changes to Microsoft Certified Professional Magazine, 2104 Harvell Circle, Bellevue, NE 68005

ABP BPA INTERNATIONAL WPA Western Publications Association

You won't get any warning that disaster is about to strike.

That's why you need Administrator's Pak 4.1.

With it, you can boot dead systems to a windowing interface loaded with powerful repair and recovery tools, easily correct mysterious registry issues, copy files from a dead system across the network, change lost or forgotten Administrator passwords, and much, much more. No matter how bad things get, **Administrator's Pak 4.1** can quickly save the day.

With Administrator's Pak 4.1, you can:

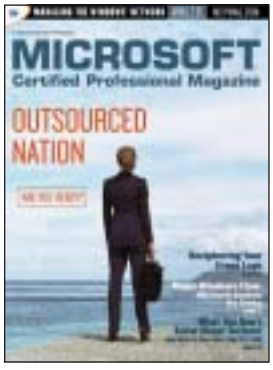
- Safely **remove viruses** while a system is offline using your preferred antivirus software.
- Change lost or forgotten Administrator passwords.
- Activate Windows XP® System Restore Points on unbootable systems.
- Access a dead system's files remotely via the network.
- Restore deleted files quickly and easily.
- Partition and format disks of offline systems.
- Quickly compare files, drivers, and configurations of dead and working systems.
- Import and export Registry keys on dead systems.
- Enable or disable services and drivers on dead systems.
- Locate and restore data from deleted or damaged partitions.

Repair. Recover. Accelerate.

Learn More!
1-800-408-8415
www.winternals.com

Winternals®

CERTIFIED MAIL



"OUTSOURCING IS A REALITY THAT EVERY SECTOR OF THE JOB MARKET HAS TO FACE."

—CHAD PIRTLE
TWINSBURG, OHIO

MCPMAG.COM MORE LETTERS FROM READERS ONLINE

RUNAS Command

I liked Don Jones' "Tips & Tricks" column, "Giving Up Privilege," in the March issue about the RUNAS command. I've been working like this since the early NT 4.0 days. As Don mentions in the column, life has gotten a lot easier since Windows 2000 and Windows XP. But there's still one thing I just can't understand. The main feature of running a program as another user is to reach files and programs with different privileges. Even though I'm fond of using the command line (I was born and raised during the DOS era), there's still some stuff that just works better with a graphical file viewer. That's were you get shocked to find out that you can run any program with the RUNAS command except Explorer.exe itself! So you can't use the best file management utility you have as another user, forcing you to log off and log on as another user to work with files. Do you know why this is? Or, do you know a good way to work around this?

—Bruno Horvat, MCSA, MCSE
Sweden

It's definitely true that you can't run Explorer with RUNAS; it won't let you run multiple instances of itself. That's an overlooked area of functionality with regard to security. What we really need is the old Windows File Manager that can run as a separate utility! In the meantime, there are third-party file management tools that may work for you (check out www.download.com for several), which you could launch under alternate credentials. Hope it helps!

—Don Jones

AD Accounts

As a fellow CISSP and reader of Roberta Bragg's "Security Advisor" column, I don't believe March's "Divide and Conquer" could have come at a more opportune time. As such, I have a best practices question regarding the creation of separate super user accounts for administration. We currently require all domain admins and higher to have separate accounts for administration purposes and one for their regular roles, per best practices. However, as it stands now, regular users who have roles such as help desk and desktop support are members of the account operators group and use their user accounts for creating such.

The question came up due to a theoretical possibility of one of the members of the account operators group logging on with normal credentials, opening an infected e-mail and creating a backdoor that captures the logon credentials. Those credentials could then be used to add or delete regular user accounts, as well as log on locally to shut down domain controllers. The credentials could also be used to delete any and all regular user accounts and groups in the domain. What are your thoughts, Roberta?

—Jack Mackenzie, MCSE:Security, CISSP
Dayton, Ohio

Yes, I believe that best practices for administrative accounts should extend to any account that has privileges that if compromised would... Well, I see from your note that you get the point. Like everything else, it's a question of risk. It sounds like you've already answered your own question. All that remains is to figure out how great the risk of such an occurrence is and what other groups of users may have a similar situation.

—Roberta Bragg

Bill's Mills

In March's "Call Me Certifiable" column, Em C. Pea asked for suggestions on where Microsoft might best put its cash reserves (now up to $50 billion) to work. You readers didn't disappoint. Here are some of the responses we liked best.

Just sign Earth over to Bill already and get it done with. Then he can come up with patches for the ozone layer as well as Windows...

—Brian S., via online
New York

How about cutting down the federal debt, so that we can thank Microsoft for unslaving us, or opening some kind of investment fund that would double all corporate donations toward that same goal—and then force aforementioned corporations into donating by not patronizing them unless they do?

Or, forget the debt. We don't seem to mind owing our souls; let Microsoft make social security solvent for all of us baby boomers by opening and running a trust fund for us.

—Carmen Arif
Garland, Texas

I think Bill's next strategy is to take over the oil companies—MS Exxon? Even Bill doesn't have enough money to buy the U.S.A. yet, but why should he when he can control it with oil and software? A gallon of gas would cost about the same as a Windows software CD—about $200. The rest of the world would be in poverty trying to buy enough gasoline to get to their job at MS Texaco, MS California or MS U.S. Congress. Of course, our children would no longer graduate from high school; they would pick from a variety of careers. MS Biologist: This person would develop new frontiers of science to integrate human life into software interests. Microsoft Money Managers: These people would provide more convenient ways of giving more money to Bill. MS Medical Doctors would sell people medication to make sure they don't rebel against the system. And, of course, there would have to be MS Prison for people like me who can't keep their mouths shut.

—Loyal Blair, MCP
Miamisburg, Ohio

It's actually very simple. Give it to SCO so they can sue over Linux.

—Timothy R. Davidson
Vail, Colorado

Outsourcing 101

In response to Dian Schaffhauser's "Editor's Desk" in the March issue, "Reality Bites," outsourcing is a reality that every sector of the job market has to face. It's a fact we have to deal with in a global economy.

What I disagree with is the idea that unions should somehow get involved. Unions have largely been the cause for much of the outsourcing in our country. They don't negotiate with the best interest of both parties in mind and, therefore, force

corporations to look elsewhere. An example is outsourcing in the automotive industry.

If unions get involved in this industry, it would be a compelling reason for me to transition to another field, not outsourcing.

—Chad A Pirtle, MCP
Twinsburg, Ohio

I'm currently employed as an accountant but was hoping to switch to the IT sector as a database developer. I'm studying to complete an MCDBA/MCSD and am horrified to read the effect that outsourcing has on the IT industry. I'm seriously considering not completing this venture, despite having spent a large sum of money on computer equipment, courses and textbooks—not to mention the time commitment.

You can imagine my disappointment to learn that this dream appears to be in danger of being snatched from in front of me, literally as soon as my efforts are poised to pay off. The idea that salaries in IT are going to collapse and the jobs themselves be exported in large numbers to countries such as India, China and Russia is devastating.

Is the honest advice to anyone in the western high-wage economies, "Don't touch IT with a barge pole"?

—Gerry
Dublin, Ireland

I don't think that domestic outsourcing and foreign offshoring are representative of the same problem. U.S.-based companies that compete with one another for the same service contracts at least are competing on a level playing field (skills, personnel, comparable education, and so on) and working from the same cost basis (cost of living, salary expectations,...). Sure, it's easy to restate the argument that some of these companies aren't entirely U.S.-based and have divisions overseas and, as such, they should have a competitive cost advantage when bidding contracts as their labor costs are less, but any short-term gain for such companies is illusionary at best and downright detrimental in the long run.

I love working in this field and was hoping it was a career that had longevity and prosperity, but, for the first time, I'm beginning to have misgivings about this concept. I imagine I'll always be able to find work as a software developer, due to proven experience with multiple platforms, languages and management experience, but I fear it just won't pay a living wage.

—Drew Wildner, MCP
Cincinnati, Ohio

There's a balanced way to do all of this. How many people changed their own oil in their car when they were younger? And now they have the dealership do it. It's cheaper to have someone do something for you. Globalization is here—you can't stop it. Yet, as a consultant, I see the limitations of outsourcing; I'm not trying to take money out of my pocket. The truth is, if you do something that most people can't do, you can't be everywhere at once. So good IT people will still have a job.

Outsoucing to offshore is another thing. There's nothing wrong with someone having a job, if he or she can do it. But can they? Communications is still a problem—not just language but culture.

—Curt Spanburgh
San Diego, California

Correction

In the Citrix MetaFrame review in the April issue, there was an incorrect reference to Microsoft LiveOffice. The correct application is Microsoft Live Meeting. Our apologies for the error.

Send Letters: E-mail: editor@mcpmag.com. Snail Mail: MCP Magazine, *Mail Editor, 16261 Laguna Canyon Rd., Ste. 130, Irvine, CA. 92618.*

Out with SUS, in with WUS

FORGET SOFTWARE UPDATE Services 2.0. It's Windows Update Services now; WUS for short.

Microsoft announced the new name and details of the overhaul of the free add-on for Windows server customers at its Microsoft Management Summit in March. WUS will enter broad beta this summer and should ship sometime in the second half of this year.

In case you've lost track, or never figured out what SUS/WUS was for in the first place, it's Microsoft's patch distribution technology for small and medium-sized organizations. Microsoft positions its patch distribution technologies in three tiers: Windows Update for consumers and very small businesses or telecommuters, WUS for small and medium-sized organization and Systems Management Server (SMS) for large or complex organizations.

WUS runs as a server in an organization. It downloads patches and updates from Microsoft's Windows Update and Microsoft Update and acts as the repository for those patches within an organization, giving administrators control over which patches are sent to end-user and server systems and when. It runs on Windows 2000, Windows Server 2003 and Windows XP.

Changes between SUS and WUS hit several important areas, including the power of the tool, the range of Microsoft products it provides patches for and its underlying architecture, which will be a foundation for the company's other patching technologies in the future.

In addition to Windows patches, administrators will be able to choose to use WUS to pull patches from Microsoft for Office XP, Office 2003, SQL Server 2000, MSDE 2000 and Exchange Server 2003. After selecting operating system and applications, administrators will have the ability to select by checkbox what types of information to download, from service packs to security patches to drivers and other things.

Initially, SUS didn't support creating target groups of systems to be updated; Microsoft chose to reserve that level of functionality for SMS. In WUS, administrators will be able to create target groups of systems for different patches. Those target groups can either be pulled from Active Directory or maintained on WUS in non-AD environments. Some limited reporting on the progress of patch installation across an organization is also being added.

From a usage perspective, WUS fills the gap in Microsoft's patching technologies between home users (served by Windows Update) and enterprises (served by SMS). But from a technology perspective, WUS is much more important. Microsoft is standardizing on the patch scanning engine that it built for WUS.

—Scott Bekker, editor, ENTmag.com

The New Microsoft Management Roadmap

LATELY, MORE AND MORE of Microsoft's planned product releases have been sliding from 2004 into 2005 or even off the edge of the map into 2006 or 2007 [Yukon, Visual Studio, Longhorn]. But for its stable of management products, Microsoft claims to still be on schedule to deliver a lot of code in 2004—at least that's what the company is saying for now.

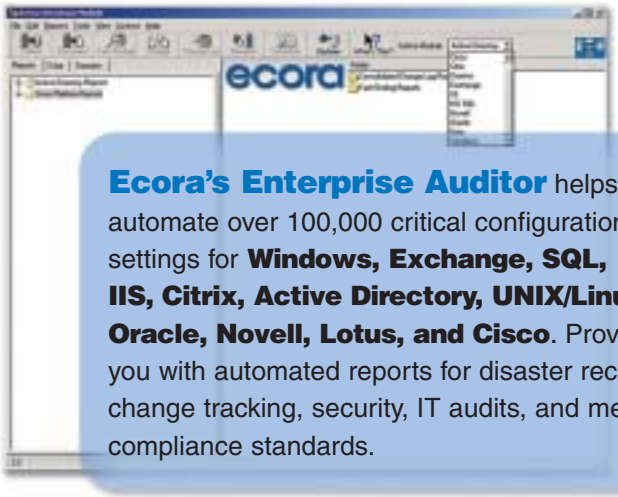
And, Microsoft officials say, don't worry about all the name changes like the renaming of the next release of Microsoft Operations Manager from MOM 2004 to MOM 2005. The product names have to do with Microsoft's fiscal year, and fiscal 2005 starts this summer. Never mind that it's inconsistent with the release of Systems Management Server 2003 in Microsoft's fiscal year 2004. Anyway, here's the roadmap that emerged out of the Microsoft Management Summit in March:

- *MOM 2005*, the management tool for monitoring IT operations, entered its third and final beta phase in March. Microsoft expects it to ship later this year, along with a new stripped-down version, called MOM Express, for smaller organizations.
- *SMS 2003 Feature Packs* are also on the way in 2004. The Device Management Feature Pack will extend SMS to mobile devices, laptops and smartphones. The Operating System Deployment Feature Pack will be designed for creating and deploying Windows OS images and for upgrading systems in place with rich status reporting.
- *System Center 2005* is a planned suite of Microsoft's two flagship management products—SMS and MOM. Microsoft says this one is coming in 2004, too, but it's dependent on some pretty clean execution. Because Microsoft plans to ship System Center 2005 with the SMS 2003 Service Pack 1 version as well as the SMS feature packs and MOM 2005, all those components must be on time for this one to make it in 2004.
- *Windows Update Services*, the new name for Software Update Services 2.0 (see above story), will enter broad beta testing in the summer and ship in the second half.

—Scott Bekker, editor, ENTmag.com

Part 11 • GLBA • Sarbane's-Oxley • HIPAA

Don't sweat it...Automate it.



Ecora's Enterprise Auditor helps automate over 100,000 critical configuration settings for **Windows, Exchange, SQL, IIS, Citrix, Active Directory, UNIX/Linux, Oracle, Novell, Lotus, and Cisco**. Providing you with automated reports for disaster recovery, change tracking, security, IT audits, and meeting compliance standards.

Special Offer: Generate your configuration reports today!

Call us at **877-923-2672** or visit **www.ecora.com/mcp** to download Enterprise Auditor and automatically generate your reports.

ecora

"Ecora Software is giving us **audit-ready reports** that show detailed configurations of our servers and routers. We just finished a major upgrade of our servers, added additional servers, and replaced our network equipment with Cisco gear. We were in the middle of the project when we were notified that we had to perform an IT audit. We were desperate for a tool that could quickly prepare us for a **last-minute GLBA audit**. Our documentation of these devices was not complete and what took us **only an hour with Ecora** would have taken weeks manually."

Karen Sullivan
Director of Information Technology
Publix Employees Federal Credit Union

A Live Meeting Minus the Airfare

Microsoft's newest collaboration tool.

BY RODNEY LANDRUM

Live Meeting (Communications Server) 2003
$375 per month for five seats
Microsoft Corp.
425-882-8080
www.microsoft.com/livemeeting

After working with Microsoft products such as Live Meeting, one becomes used to the term "wholly owned subsidiary." Live Meeting, a Web presentation service acquired from PlaceWare, is similar to Live Communications Server 2003, sold under the Office umbrella.

While the two products are quite different in presentation, both offer online collaboration, discussion, application sharing and archiving, along with many other features that use Real Time Communication protocols. Live Meeting promises to be most beneficial to customers that need to participate in a meeting or presentation outside of their organization. Live Communication Server 2003, meanwhile, is more suited for enterprise employee-to-employee (E2E) collaboration.

Because Live Meeting is currently a service and not an installable server application, I signed on for the 15-day trial, which allows presenters to schedule meetings and invite other participants to attend over the Internet. The invitees don't need to sign up, but do need to download the Live Meeting Conference Center application.

The presentation section of Live Meeting can contain various types of slides, including PowerPoint, Whiteboards and Web pages.

After completing the online registration form, I got an e-mail on how to log in to the Live Meeting site to schedule my first meeting. Anxious to get going, I went to the main login page, and from the main menu had several options to schedule and manage meetings. I set one up called "Recording Meeting" and sent out the invite.

There are several ways to communicate with the audience. For instance, a chat client is built right into Conference Center.

As I inserted various types of slides, such as a Whiteboard slide and Web slide, they were immediately visible to the audience. The Web slide was especially useful as the entire Web site is loaded in and can be navigated just as within a browser. These slides can also be referenced at any time—perfect for an informal brainstorming session.

Using Live Meeting in conjunction with a teleconferencing provider for real-time voice input is where the real power of the service comes in. The audience can indicate that they have a question, and their status color will change. Even without voice capability, the audience member could type the question into Conference Center, and the presenter can answer it at the appropriate time.

The ability to record Live Meeting sessions, including audio, and then rebroadcast is a great feature. To record audio, the Conference Center system where the presentation is being given also needs to dial into the telephone conference call system.

The more I worked inside of Live Meeting, the more I realized this service could have far-reaching benefits for customers and employees, from remote training and support, to company meetings for the traveling sales force.

There are several pricing options from a flat fee of $375 per month to time-based usage, which is 35 cents per minute. Though $375 may seem steep for many companies, when you think of the cost of travel and time, it can more than pay for itself.

Rodney Landrum, MCSE, is a data analyst and systems engineer for a software development company in Pensacola, Florida. He's at rodneyl@healthware.com.

Paging the Help Desk

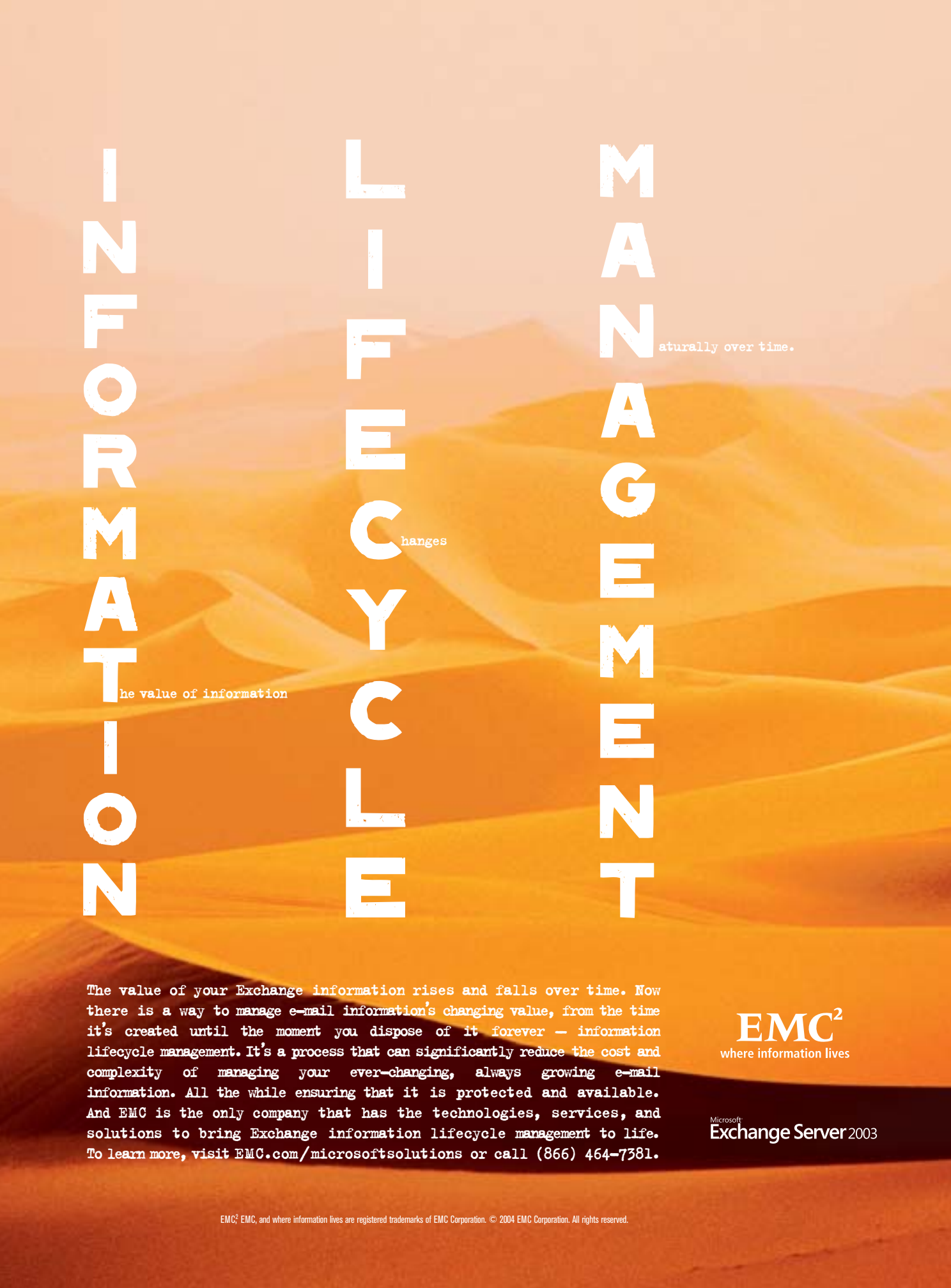
TRUE LIFE TALE

Submitted by Dana Cummins

I was new with the desktop support team and received a request to take a look at a customer's computer that was making a funny noise. I went on site and asked the user, "What kind of noise?" All she could say was that it was making a buzzing noise and it was coming from the keyboard. Surprised by this description, I sat down at the keyboard and began doing some basic troubleshooting when, all of a sudden, I heard the sound. It was definitely coming from somewhere near the keyboard, but it was a sound I've never heard before from a computer.

After further investigation of the area, I pulled the center drawer of her desk open and—voila!—there was a pager in the drawer, set on vibrate. When I told the customer that it was a pager located in her center drawer, her comment was, "There it is. I've been looking for that for weeks!"

For her tale, Dana received Mastering Windows XP Registry, *courtesy of Sybex. Submit your tale to: editor@mcpmag.com.*


INFORMATION
The value of information
LIFECYCLE
changes
MANAGEMENT
naturally over time.
The value of your Exchange information rises and falls over time. Now there is a way to manage e-mail information's changing value, from the time it's created until the moment you dispose of it forever — information lifecycle management. It's a process that can significantly reduce the cost and complexity of managing your ever-changing, always growing e-mail information. All the while ensuring that it is protected and available. And EMC is the only company that has the technologies, services, and solutions to bring Exchange information lifecycle management to life. To learn more, visit EMC.com/microsoftsolutions or call (866) 464-7381.
EMC²
where information lives
Microsoft
Exchange Server 2003
EMC², EMC, and where information lives are registered trademarks of EMC Corporation. © 2004 EMC Corporation. All rights reserved.

Share and SharePoint Alike

Managing and sharing documents the Microsoft way.

BY RODNEY LANDRUM

SharePoint Portal Server 2003
$3,999 per server,
$71 per device or user
Microsoft Corp.
425-882-8080
www.microsoft.com/sharepoint

SharePoint Portal Server 2003 is now a Microsoft Office 2003 product and shares the spotlight with a sister technology (more like a Siamese twin)—Windows SharePoint Services (WSS), included with Windows Server 2003.

I installed SPS 2003 on a Windows 2003 system running SQL 2000 SP3a. You have the option of installing MSDE as the database engine instead of SQL Server. The installation took a little time as it had to create the databases and the initial portal site, but otherwise it was straightforward and flawless.

I launched my browser, typed in the server name where SPS was installed, and was able to access the default site (in essence my organization site) where sub sites and workspaces could be created. I made a site for my department called Engineering, where I'd do the bulk of the work.

If SharePoint is installed with default Web settings, the software is set up in the root of that Web, so that you type the server name to get to the main site. It's possible to change this behavior by creating a new site and installing SharePoint there.

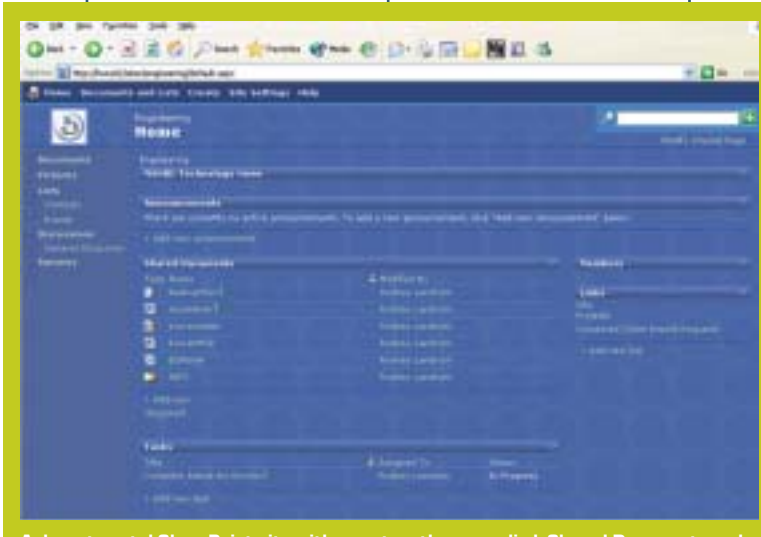
Administrative tasks can be doled out at the site level or rolled up to the main site in the hierarchy. Having the ability to consolidate, index and manage multiple SharePoint sites—say for engineering, sales and development that may be on separate systems—is one of the benefits SPS offers over Windows SharePoint Services.

SPS creates centralized document storage areas that makes finding information easier. With that in mind I wanted to try out the indexing and search features first. I could either index content sources that existed outside my engineering site, such as file shares, or import documents directly into the site. I chose to import to see how easy it would be to load multiple files, and because I could be selective about which files to move. As the figure shows, I was able to move in five files at a time. I did this in the Shared Documents location, though I could have just as easily made another document area. One problem is importing multiple files; you can only import multiple files from a single folder. There are external portal tools that let you move many files in programmatically.

After a working set of files is created or uploaded to the site, members have many options for collaborating. Custom "workspaces" can be created when the document is opened, say, in Word or Excel, where team members can meet to discuss and work on the document. Using Windows Messenger adds real-time collaboration, and the online status of other team members is also available inside Office 2003 applications.

One great feature is the ability to set alerts when the document changes. These can be set to send mail immediately or on a schedule.

For all that SharePoint offers in making document management and collaboration much more efficient, it does require a change in thinking. Many people are accustomed to searching for files in a hierarchical folder structure imposed by the file system. With SharePoint, users will work from within the portal, searching for and managing content at their department level or personal workspace. I had to overcome several obstacles when using SharePoint, but these obstacles were more in changing the way I work. Sending a link to a document from the portal is not as simple as a click of the mouse, and the link to the documents became rather large and unwieldy, using "%20" for space character substitution. In addition, when large amounts of content are added to document libraries, they can easily become just as difficult to sift through when looking for a particular document. All in all, SharePoint is a great collaborative foundation for companies, and I recommend utilizing its many features with Office 2003 applications.



A departmental SharePoint site with a custom theme applied. Shared Documents and Tasks can be added anywhere to the site.

Rodney Landrum, MCSE, is a data analyst and systems engineer for a software development company in Pensacola, Florida. He can be reached at rodneyl@healthware.com.

Keeping Pace With Patches

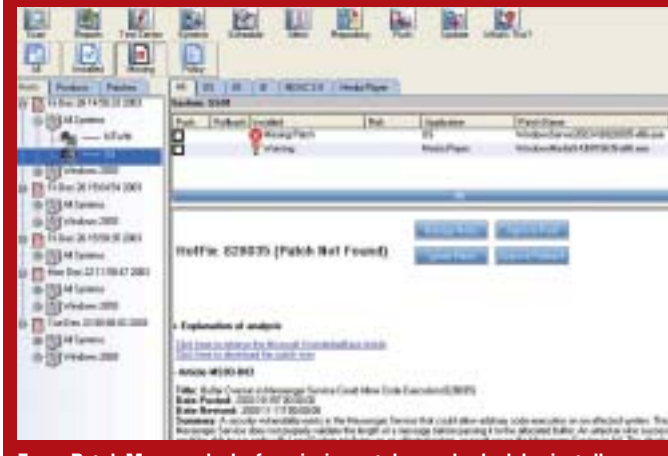
Ecora automates Windows and Unix patch management.

BY RODNEY LANDRUM

Ecora Patch Manager 3.0
Prices start at $50.70 per node
Ecora Corp.
603-436-1616
www.ecora.com

It only takes one vulnerable machine and one attack to make a system administrator's day go horribly wrong. That's why patching is so important, and why I was glad my editor asked me to look at Ecora Patch Manager 3.0, which I ran on my Windows XP Professional system. (The company has since begun shipping version 3.1.)

Ecora has a Web licensing service that provides the license after installing and running the application for the first time. I stepped through the configuration screens, providing information for each of the various components that make up the product: SQL Server database to store the system and patch history information, a local shared repository location to keep local copies of downloaded patches, and the Web Reporting Center. I was unable to install the Reporting Center during the initial setup (explained later, and involving a call to tech support), so I continued the install, thinking I'd resolve the issue later. I was anxious to get patching.



Ecora Patch Manager looks for missing patches and schedules installs.

Patch Manager provides a single location for performing the tasks necessary to patch a network. From the Patch Manager main console you can scan systems, schedule scans and patch installations and search the repository.

Now it was time to add systems to the Patch Manager database. This can be done several ways, the easiest of which is to "discover" the systems. I checked a Windows Server 2003 system and an XP Pro workstation for hotfixes, as I knew these machines wouldn't have the latest hotfixes applied (don't tell my boss). Once I discovered these systems—a straightforward process by choosing the domain and system names from a list—I scanned them for missing patches. Patch Manager successfully connected and scanned both systems quickly. In the time it took to scan only two systems—about 15 seconds—I concluded that my entire network could be scanned on an evening schedule in under 10 minutes.

I noted one system, my Windows 2003, was missing a specific hotfix, KB828035 to be exact; it fixes an issue with buffer overruns in Messenger. To test the validity of this finding, I went out to Windows Update and manually reviewed what critical updates weren't applied. I saw that no critical updates were available from Windows Update. Hmmm. I reviewed my installation history on Windows Update and discovered that this update had been applied already, back in October. Was Ecora misreporting this patch? Not at all: Patch Manager was aware that this patch had several revisions and I didn't have the latest version.

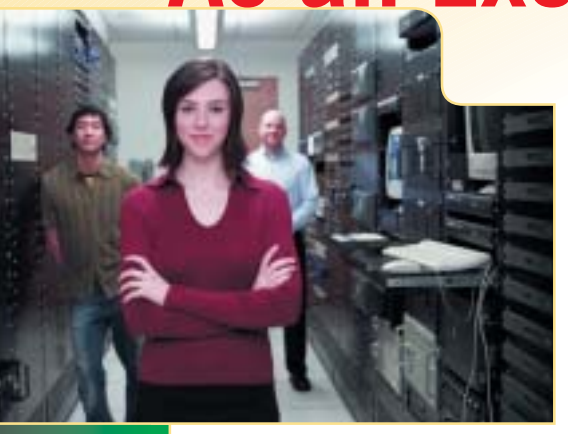
I mentioned earlier an issue with installing the Reporting Center. Of all of the components to install, this was one I'd decided to install remotely, not on my XP box with all the other pieces. Subsequent installs of Reporting Center failed on the Windows 2003 IIS machine. I called technical support about this along with another issue concerning the Help screens displaying a blank form. I'm happy to note that a subsequent installation of the product fixed both issues. Support answered the phone in less than two minutes on every call, even the day after Christmas. With Reporting Center functional, I was able to view all the patch installations through the browser and filter the reports off of system groups, which is a nice feature for larger organizations.

There are enough features in Patch Manager 3.0 to make it a worthwhile investment. Centralized administration, superb auditing and reporting and instant access to information about all available hotfixes makes it a strong contender. Patch Manager 3.0 is relatively new and there are features I'd like to see added, like having a history automatically displayed in the main console without having to load in saved scans after each launch. Also, many of the dialog boxes are a little too heavy on the tooltips, which inundated me with yellow popups endlessly when trying to discover systems. An example: If I didn't know that the Cancel button would "close the dialog box without saving or implementing changes," maybe I shouldn't be the one patching systems.

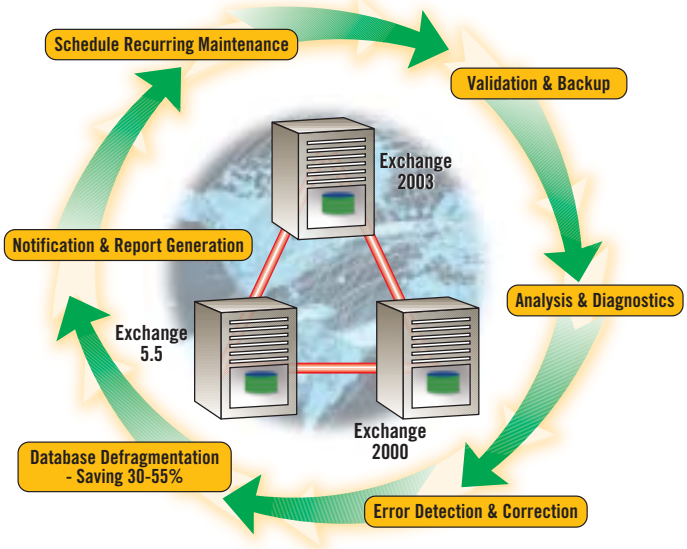
Overall, Ecora Patch Manager 3.0 was impressive, and has an advantage over Windows-centric patch management offerings: It also patches many Unix systems. Until Windows Update can do that, which will be never, Patch Manager will have a leg up on SUS and other security patch products—even if they're free.

Rodney Landrum, MCSE, is a data analyst and systems engineer for a software development company in Pensacola, Florida. He can be reached at rodneyl@healthware.com.

As an Exchange Administrator,



New Version 3.0



As an Administrator, your Exchange servers are mission critical... and **FAILURE** is **NOT** an option. Your Exchange systems experience **ENORMOUS STRAINS** behind the scenes and without proper maintenance, **DISASTER** may strike at any moment.

Lose Exchange and Your Going Down!

Without Exchange, you're invisible to the rest of the world and you can kiss your companies productivity goodbye. You may as well turn out the lights, send everyone home, and cancel your personal plans. It's going to be a long night.

So, How Do You Protect Yourself?

You have more important things to do with your time than participate in the never ending battle of keeping your Exchange server maintained, especially when it's a war that you can't win – not on your own anyway. Which is why we created **GOexchange**, the "Automated Maintenance Solution for Microsoft Exchange 5.5, 2000, and 2003".

Exchange Database Before

100 GB

- Degraded performance
- Questionable stability
- Bloated message store
- Erratic and strange behavior
- Multiple errors and warnings
- Deleted items still intact

Exchange Database After

62 GB

- Optimized message stores
- Reduced store size by 38%
- 1557 errors removed
- 232 warnings corrected
- Increased performance & stability
- Deleted items completely removed

From the **GOexchange** Centralized Management Console, you now command the ability to configure, manage, schedule, and review preventative maintenance *for all of the Exchange servers within your organization to…*

Prevent Disasters: Minimize unplanned downtime and prevent disasters caused by unstable and inefficient databases.

Repair Problems: Expert knowledge for Exchange is built-in to check and correct errors and corrupted objects.

Accelerate Performance: Databases are re-indexed and defragmented to permanently remove white space and deleted items. The end result is increased performance and stability with a compact efficient database that's 30 to 55% smaller.

Best of all, it's EASY. – *Just Click GO!* >>>

Failure is Not an Option.

GOexchange is Your Automated Maintenance Solution.

Leverage the powerful features of GOexchange and Get Your Life Back…

Centralized Management, Scalable, and Easy to Use

With its centralized management console, and robust architecture capable of scaling to hundreds of servers and its superior ease of use, GOexchange can quickly address the demands of even the most dynamic IT environments.

Scheduling and Notification

Schedule jobs for any server within your organization to automatically take place on specific days, times, and intervals. Notify specific persons, all members of a group, or the entire organization of an upcoming or completed maintenance. *GOexchange works 24x7x365 so you don't have to!*

Advanced Concepts and Configuration

GOexchange understands advanced concepts like clustering, and you can configure a job to maintain a server, targeted individual stores, or groups of stores.

Security

GOexchange takes full advantage of Microsoft's security model to ensure that only authorized Exchange Administrators have access to its powerful features.

Backup Integration

Run a backup job before and after maintenance with solutions from CA, VERITAS, UltraBac, CommVault and more.

Reporting

Detail and summary maintenance reports by server or job name.

Microsoft CERTIFIED Partner

Provides Piece of Mind "GOexchange removed an incredible amount of errors and significantly reduced the size of our databases. If you want to keep Exchange optimized and running well, this is a tool Exchange Administrators really can't afford to live without. Most important GOexchange provides us with piece of mind."

Andy Jacobs
Sr. Messaging Administrator
BlueCross BlueShield

Uptime and Availability: "After just one use of GOexchange, our information stores were reduced by 45-50% with thousands of errors, warnings, and inconsistencies corrected. Without GOexchange we would be unable to provide the current level of 99.999% uptime and availability to our customers."

Dale Huitt
Network and Systems Administration Team Lead
State of Oregon - DAS OIT

"We Rely on GOexchange. Life before GOexchange was challenging at best, and some days it was an absolute nightmare, late nights, long weekends and upset users. Our firm has relied on GOexchange for maintaining Exchange for over three years. Our faith is well placed, as we have not had a single issue with the Exchange server since."

Pamela Olson
Network Administrator
Levinson Friedman

GOexchange
AUTOMATED MAINTENANCE

See for yourself – Download your FREE 3.0 demo version now at: www.GOexchange.com 425.451.2595

Why Do Spammers Spam?

SPAMMING IS A LUCRATIVE business that can be started up for a ridiculously small amount of money. And in the end, spammers are mostly misunderstood individuals who are providing a valuable service. So they say.

Those are some of the conclusions from a special report published by anti-spam vendor Vircom. The report, "Why Spammers Spam", sheds some light on the shadowy world of junk e-mailers. By agreeing not to reveal any information about them, including their real or online names, and printing their responses to questions verbatim, Vircom was able to entice three spammers to talk about their industry.

"Virginia," a 19-year-old college student, started spamming to help pay for tuition. She said "...all I had to do was invest in a new Internet provider, and buy a list of e-mail addresses. I started up for pretty much nothing and turned a profit on the first day!" According to Vircom, "Most spammers can get started for under $1,500 and may earn back their initial investment within a few days."

As to the types of products they peddle, Virginia says she's had success with low-carb diet plans and discount travel. "Thomas" says, "I have peddled everything from diet pills to porn. I usually get the biggest response from porn."

To make sure their spam gets through, Thomas says, "I use two spam filters; one is open source that I downloaded for free, and the other is an enterprise copy of a commercial filter." Virginia uses the spam filter in her father's office. "If I can get through it, then I can get through most spam filters."

The spammers interviewed have a remarkable ability to minimize, in their minds, the impact their work has on businesses and home users. Answering the question, "What are the costs to the public from spam?" "Matt" answers simply, "Nothing." Matt also doesn't think the government's efforts at controlling spam are working. "Right now, the U.S. government has had zero results in controlling spam. Perhaps if they review some of its problems, then it will have an effect."

Especially revealing were answers on whether the spammers worry about the recipients who get their messages. "The possibility of children being exposed to certain types of messages weighed upon all of the participants, but they all maintain a distant, almost detached outlook," Vircom states.

Virginia said she does worry. "Definitely, that is why I will never market porn," she says. Matt has no such qualms. "I have peddled flesh in the past, and will do it again. I am not going to lie and say that I am above that. The fact is that skin sells!"

A copy of the report can be obtained from www.vircom.com.

—Keith Ward

Sun, Microsoft Kiss and Make Up

SUN CEO SCOTT MCNEALY says that customers drove Microsoft and Sun to the reconciliation that created a 10-year partnership pack aimed at Sun/Microsoft interoperability. But the real reasons are anybody's guess.

Let's face facts. Sun is facing down a critical loss of overall momentum and Solaris market share in particular, 3,300 layoffs, and a loss of up to $810 million for the third quarter—not exactly a prime negotiating position. Microsoft, meanwhile, is facing $613 million in anti-trust penalties from the European Union, charges that Sun (and Netscape) did much to fuel.

So perhaps in pure mutual self interest, the two giants concocted a deal where Sun gets a nearly $2 billion payout to cover anti-trust and intellectual property issues, and both parties agree to broad cooperation on interoperability.

In a mind-warping press conference, former Microsoft-basher McNealy promised to "be good" and both he and Microsoft CEO Steve Ballmer pledged their deep and undying friendship.

But the big story is the result this promises for IT. It's not just an end to the bickering, though the nasty and cruel back and forth was getting tiresome. It really means that it will be easier to blend Sun and Microsoft technologies, whether they be discrete Windows or Solaris servers or full-blown development environments such as Java and .NET.

In those respects, the companies agreed to:

- *Share technology*. Both agree to share details of server technology to help insure interoperability. This includes core server OSs, major applications such as messaging, and eventually new identity-based initiatives.
- *Protocols*. Sun will license Windows desktop protocols, which will ease the interoperability of Sun and Microsoft client OSs and apps.
- *Java*. Microsoft is free to support its widespread Java Virtual Machine.
- *Windows and Sun*. Microsoft will certify Sun Xeon and eventually Opteron-based servers as Windows-ready.

Regardless of motives, this agreement is a boon to customers (and antidote to Sun's market woes and Microsoft's anti-trust problems), who will be able to choose the server, application or development technology that serves them best, without obsessing over whether it will work with already-installed pieces.

—Doug Barney

MCP CERTIFICATIONS

MCP	963,606
MCP+Internet	229,139
MCP+Site Building	2,040
MCSA (Windows 2000)	104,703
MCSA (Windows Server 2003)	11,314
MCSA: Messaging	15,499
MCSA: Security	2,091
MCSE (Windows NT)	394,807
MCSE (Windows 2000)	244,153
MCSE (Windows Server 2003)	5,604
MCSE+Internet	12,456
MCSE: Messaging	3,082
MCSE: Security	2,505
MCDBA (SQL Server 2000)	122,586
MCAD (VS .NET)	15,769
MCSD (VS 6.0)	45,150
MCSD (VS .NET)	7,744
No. of Certifications	2,182,248

Numbers indicate total certifications per title as of April 14, 2004.

Control Schizophrenia

FSLogic Protect 1.0 supports multiple personalities.

BY MATT KINSEY

Protect 1.0
Prices start at $80 per user
FSLogic/Altiris
801-226-8500
www.fslogic.com

So you just left the local copy shop after printing out a revised sales presentation when you suddenly realize the confidential file is still on their computer system. Is it time to panic? Not if the shop is using FSLogic Protect.

FSLogic Protect 1.0 (recently acquired by Altiris) is designed to safeguard multiple-user access and public use computers, such as those found in copy shops, Internet cafes and libraries. It's also perfect for PCs shared by traveling salespeople, consultants, or corporate visitors. Instead of locking down these computers, Protect allows users to control their own experience and configuration. Each user can change their own preferences or settings, and save or delete files without placing other users' information or settings at risk.

Protect works by storing all changes made during a session in its own "File System Layer." This layer keeps track of all Registry, file and configuration changes so they can be saved, archived or deleted upon the end of a session. Once the user logs off, the PC is restored to its original setting without rebooting.

Protect also offers discrete control over multiple user sessions. The software can be configured to either protect or not protect a user's session. If not protected, all changes made in that session are applied to the original installation. This way, administrators can apply security patches and make configuration changes. If the session's protected, the administrator has the option of archiving the user's session, leaving the session on the computer or removing it. If the session is removed, all changes associated with it are also removed.

One really nice feature of Protect is the ability to migrate a user's session from one computer to another—this way the star traveling salesperson can have the same experience, no matter which PC he or she takes over. And profiles can be stored on a network location so the users will get their same desktop experience when moving across PCs.

Protect only works with Windows 2000 and newer operating systems using NTFS formatted disks. System requirements are equivalent to the OSs for memory and processor; however, file storage requirements need to be taken into consideration. The more sessions left on the computer, the greater the amount of disk space needed.

The test bed on which I tried out Protect consisted of a 512MB 2.8MHz machine running Windows 2000 Professional, Win2K Server, XP Professional and Windows 2003.

Installation and configuration is straightforward, although it does require a reboot. The first step is to configure the administrator, which defaults to the local administrator. Users are grouped by the PC's local groups. In an Active Directory environment, you can protect users by adding global groups to the local groups.

The Configure console in FSLogic makes it easy to choose whether or not to protect a user, and what to do with an unprotected session.

After configuring the administrative user and defining a test folder to exclude, it was time to configure the users. For each user, the administrator must define whether to protect the user or not. If the user's protected, the administrator must also define whether the changes will be archived to a network location, stored locally or discarded upon session termination.

Testing results were exactly as advertised. In controlled tests, a series of configuration changes were made under various user profiles. These changes included software installations, Registry changes, saving files and other configuration changes. Snapshots of the Registry and file system were taken before and after the installations to verify the results. In all cases, Protect performed as instructed. Protected sessions were deleted, archived or saved based upon the configuration. Non-protected sessions were applied directly to the underlying OS. Additionally, Protect successfully imported a session from another system and applied the changes seamlessly.

Protect is worth a look in public-use computing areas such as mall kiosks and schools using Win2K and newer OSs. In corporate environments, the software would offer benefits to call centers, lab environments and other areas that house open-access PCs.

Matthew A. Kinsey, MCSE, MCSE+I, CCNA, holds a master's degree in Computer Information Systems and is currently an MIS consultant for a major retailer. Contact him at mattkinsey@bellsouth.net.

Who's guarding your Exchange Server?

Fifi = a single anti-virus engine!

Buster = the real thing!

Get the leading email content security & anti-virus solution!

GFI MailSecurity

Email content/exploit checking, anti-Trojan & anti-virus

If you are serious about mail server protection, get the leading email content security, anti-Trojan and anti-virus solution, **GFI MailSecurity for Exchange/SMTP**, the only product to offer these unique features:

- **Multiple virus engines** – For better security
- **Email content & attachment checking** – Quarantine dangerous attachments and content
- **Email exploit protection** – Perform email intrusion detection and defense
- **HTML threats analysis** – Disable HTML scripts
- **Trojan & Executable Scanner** – Detect potentially malicious executables
- **Server-based anti-spam** – with the GFI MailEssentials bundle!

NEW PRICING!
Only $315 for 25 users; $950 for 100!

– Used by customers like NASA, Caterpillar, European Central Bank, MG Rover Group, Toyota & many more

Download your FREE trial from www.gfi.com/sec

GFI NETWORK SECURITY
CONTENT SECURITY
MESSAGING

tel: +1 888 243 4329 / +1 919 388 3373 | email: sales@gfi.com | url: www.gfi.com/sec

Souping Up Windows 2003 Migrations

By Danielle Ruest and Nelson Ruest

We review five tools that speed and ease Windows 2003 file and print migrations.

MIGRATING TO WINDOWS SERVER 2003 from either Windows NT or Windows 2000 Server must be done carefully—and in the right order. That's why most migration projects involve a minimum of four migration steps:

1. Migrating security principals
2. Migrating member servers
3. Migrating PCs
4. Migrating applications

We tested five tools to see which ones provide the most bang for the buck.

Quest Consolidator

Quest Consolidator (formerly FastLane Consolidator) in-cludes two basic components: a client and a server. The client is designed to install on source servers to perform migration operations as dictated by the server component. The server includes a central migration database along with migration schedules. Supported databases include Microsoft SQL Server Desktop Engine or SQL Server. Migrations can all be run from the server, so clients are completely optional. Consolidator is composed of two elements: the actual consolidation tool and a storage analysis reporter. This fully supports the consolidation process because the Storage Analysis Wizard reports on file usage, file duplication and file ownership.

The Consolidator interface is clean and easy to use (see Figure 1).

The startup screen displays all the tools you need to support migrations and consolidations. The first tool is the Storage Analysis Wizard. Once your data patterns have been analyzed, you can proceed to a migration/consolidation. Data and print migrations are simple: just run the appropriate migration wizard. In addition to data and print migration, the Consolidator startup screen gives you immediate access to three utilities: Home Path Updater, Profile Updater and Printer Migration. The latter is, oddly, the same as the Migrate Printers item in the center of the startup screen. But the first two utilities are really useful. They support the update of user profiles to point to new home directories, remote profile paths, drive mappings, desktop shortcuts and even object linking and embedding (OLE) in Microsoft Office documents. Printer migrations are supported by a RegTool utility that lets you change printer mappings on client computers through a logon script.

One of the product's greatest assets is that it allows testing of a migration before it's performed.

In short, Consolidator worked well and provided an easy path to migration and consolidation of both file and print servers. Some drawbacks are that it works only with home directories and doesn't seem to offer any direct support for folder redirection. The same goes for the Distributed File System; Consolidator supports the migration of drive mappings, but though it

Figure 1. Quest Consolidator sports a clean interface outlining the three steps to a migration or consolidation: analyze data, migrate or consolidate data and migrate or consolidate printers.

MCPMAG.COM
The online version of this article includes the full test plan and environment, tips on migrating data and loads of additional resources.

Illustration by Ryan Etter

may support the modification of a user mapped drive to a DFS map, it isn't immediately self-evident how this should be done. Finally, printer migration is direct—that is, it migrates printers with existing drivers and doesn't change kernel-mode printers to user mode.

Aelita Consolidation Manager

Consolidation Manager (CM) also works with two basic components: a central server that stores the migration database and hub servers that actually run the migration jobs. This distributed architecture gives you control over both the bandwidth used in your migration and the amount of processing power assigned to the migration process. Migrations are run as jobs (see Figure 2).

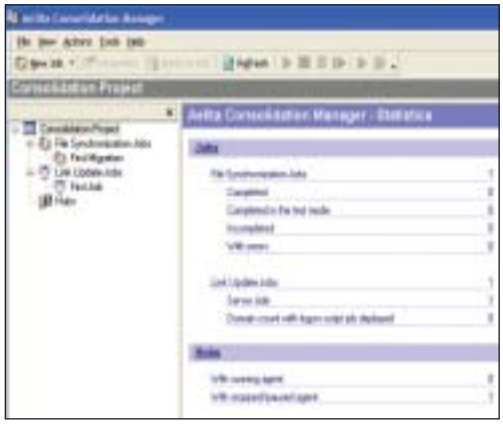


Figure 2. Aelita's Consolidation Manager operations are based on the "job" concept: define a migration job and run it. Once the file synchronization job completes, you can run link update jobs.

Figure 3. Small Wonders' Secure Copy interface is easy to use. Just follow three steps and you're ready to copy. Identify the source, the target and set your options.

You begin by defining a file synchronization migration job and running it. Next, you can run link update jobs. Jobs can be tried in test mode to determine if they'll actually work before being run.

File synchronization jobs are transparent to users because you can run both the source and target server in parallel and update client components only when you're ready to decommission the source server. CM updates home directories and profile paths through the Domain Directory wizard. This wizard also updates shared folder and printer information in Active Directory domains. The Link Update wizard updates components located on member servers or client workstations such as OLE links in Microsoft Office files, shortcuts and mapped drives as well as printer references.

Printer migrations are run through the Printer Migration wizard, though strangely this tool is hidden inside a menu rather than being directly available through the CM interface. Print migration jobs are comprehensive. They include printer properties, drivers, ports, page separators, print forms, color profiles, and even print jobs, though the latter don't work from NT boxes.

Though CM does most everything required for a migration or consolidation, it doesn't directly support Windows 2003's most advanced features such as folder redirection instead of home directories and DFS shares instead of mapped drives. CM can be used to target these features, but you'll need to write special scripts to add to file synchronization jobs. The advantage is that CM provides very powerful scripting support in either VB or JavaScript. Overall, CM is easy to use and provides a powerful file and printer migration toolkit.

Small Wonders Secure Copy

Secure Copy is different from both previously reviewed tools. It's designed specifically, and solely, for the migration of files and folders from source servers to target servers. Its installation is simple, using an MSI package that provides two installation choices: complete or custom. For some reason, there's only one component to choose in the custom option. But once installed, Secure Copy is really easy to use. It offers a no-

Product Information

Aelita Consolidation Manager, version 6.0
Starts at $1,099 per server
Enterprise Directory Reporter, version 5.1
Starts at $8 per user account
Aelita Software
614-336-9223
www.aelita.com

Consera AgileOne, Version 2.1
Starts at $659 per managed server
Solution Builder starts at $6,000 per developer
Hewlett Packard (recently acquired Consera)
425-867-5300
www.consera.com

Ideal Migration Version 3.0
Starts at $169 for 1 to 50 users
PointDev
33 4 32 62 71 34 (France)
www.pointdev.com/IM_descr_us.htm

Quest Consolidator 4.1.2
Starts at $995 per server
Quest Software
949-754-8000
www.quest.com

Secure Copy Version 3.6
Starts at $598.80 for a single server license with one-year maintenance
Small Wonders/ScriptLogic
561-886-2400
www.smallwonders.com

nonsense interface allowing easy access to all features (see Figure 3).

Secure Copy also works with jobs. Job creation is a simple three-step process: identify the source, identify the target, set your options and away you go. Options include what kind of files to copy; for example, only changed files; permission copying options such as resetting user passwords when accounts are migrated; file compression options; file share migration options; local group copying options; and file filters to use for copying. Secure Copy automatically copies local groups and user accounts, and even targets specific organizational units in AD during the copy. Copy jobs can be tested prior to the actual copy to ensure they'll work properly.

Secure Copy does almost everything required to transfer files with security settings from one server to another. It doesn't, however, provide any tool for the modification of user settings or file references on local computers. For this, you'll have to make your own scripts or batch files. It also doesn't migrate printers at all because it's a file copy tool. Finally, it doesn't include a reporting tool to help in the archiving of obsolete or unused data. But for file copying, Secure Copy performs as expected, making server consolidation easy.

PointDev Ideal Migration

Ideal Migration is designed to manage all migration tasks, from domain migration to user settings and passwords. It's an MMC, installable on all versions of Windows server from NT 3.51 forward (see Figure 4).

As such, it fully supports the concept of migration delegation. It's simple to install, but doesn't use an MSI installation. Its migration strategy is simple: export data and objects from one location and import into another location.

Figure 4. PointDev's Ideal Migration supports domain, account, file server and printer migrations through the use of very simple dialog boxes. Migrations can be stored in projects and run as scheduled tasks.

Migrations can be performed by selecting the objects to migrate in the left pane, right-clicking on the object and selecting the object type migration from the context menu. In the migration properties dialog box, identify the source or export server, then identify the target or import server. Objects are migrated with complete security set-

Figure 5. Consera's AgileOne provides both migration and consolidation services through a simple series of steps, all from a remote console.

tings. Migrations are performed by exporting data to a .csv file, which is then imported. To perform file server migrations, first perform a shared folder migration, then a file and folder migration; these can be grouped together in one step. Migration properties can be stored into project files that can be run later through either scheduled tasks or the command line. This gives Ideal Migration a lot of flexibility.

Printer migrations are performed the same way as file and shared folder migrations—simply point and click. But there are caveats: printer driver migrations must be from the same OS to the same OS—for example, NT to NT or 2000 to 2000—otherwise, they must be installed manually beforehand.

The main failing of Ideal Migration is the absence of reporting tools; you can't see what to eliminate from your migration. This would make it impossible, for example, to send unused files to archived storage. Other than that, it's easy to use for all the object type migrations it supports. It may, however, be overkill if all you need is to perform a file and print migration. But if you need to migrate more than just file and print, it may be the right solution for you.

Consera AgileOne

AgileOne is a unique product in this space. That's because it's really an extension of Microsoft's Automated Deployment Services (ADS)—an enterprise server deployment system. This limits Agile-One's accessibility, because ADS is only available to organizations that have volume license agreements with Microsoft. ADS provides a complete set of tools that facilitates the server provisioning process in any datacenter. It lets you capture base server installations and redeploy them from a central location. It'll even let you provision servers that have nothing installed on them, all from a remote location! ADS is powerful, but it relies heavily on command lines and XML scripts.

In terms of file servers, AgileOne will let you capture a file server's "profile" and restore it to any other server in your enterprise. This means that AgileOne supports both file server migration and consolidation, all through a point-and-click Web interface (see Figure 5)—pretty nifty. AgileOne also provides three additional functions: graphical interface to ADS, ADS process automation and graphical server provisioning extensions.

In terms of Automated Deployment Services, AgileOne provides graphical functionality for most ADS commands, including server discovery, image capture, and image deployment. Second, it automates most tasks you'd need to perform manually with ADS (for example, the installation of the System Preparation tools on remote servers). In addition, AgileOne automatically deploys the ADS agents during its server discovery process.

For file server migration, AgileOne supports server personality transfers, as

Table 1: Migration Tool Evaluation

Activity	Quest Consolidator	Aelita Consolidation Manager and Enterprise Reporter	Small Wonders/ ScriptLogic Secure Copy	PointDev Ideal Migration	Consera AgileOne
File Migration	✓	✓	✓	✓	✓
Print Migration	✓	✓		✓	
Consolidation Support	✓	✓	✓	✓	✓
Source Operating Systems	NT, 2000, 2003, EMC Celerra, NetApp Filers	NT, 2000, 2003, Novell, NAS	NT, 2000, 2003	NT, 2000, 2003	NT, 2000, 2003
Target Operating Systems	NT, 2000, 2003, EMC Celerra, NetApp Filers	NT, 2000, 2003, NAS	NT, 2000, 2003	NT, 2000, 2003	2000, 2003
File Usage Analysis before migration	✓	With Enterprise Reporter			
File Re-ACLing	✓	✓	✓	✓	✓
Password Protected File Support	✓	✓	✓	✓	✓
Parallel File Server Support	✓	✓	✓		✓
Support for Single Instance Store					
Support for Windows Storage Server 2003	✓	✓	✓	✓	✓
User/PC Setting Migration	✓	✓		✓	
Undo Capability				✓	✓
Delegation of Migration Task	✓	✓		✓	✓
Migration Reporting	✓	✓	✓	✓	✓
Migration Testing	✓	✓	✓		✓
MMC TaskPad	✓	✓		✓	Web Interface
MSI Installation	✓	✓	✓		✓
Database Support	SQL or MSDE, versions 7 or 2000	SQL or MSDE, versions 7 or 2000			SQL or MSDE, version 2000
Scripting or Command-line support	✓	✓	✓	✓	✓
Documentation Format	PDF, Compiled Help	PDF, Compiled Help	Compiled Help	Word, Compiled Help	Compiled Help
Tutorials or Quick Start Guides	✓	✓		✓	✓

it's designed to work with server roles assigned after OS installation. AgileOne captures and transfers file server settings—even settings based on Distributed File Services. This means it supports both server transfers and server consolidation, because it emulates the legacy server's NetBIOS name on the target server to ensure that users don't lose file access during the transfer. Very powerful, indeed.

One of its neat features is the automatic reversal of all operations in the case of error. This ensures the constant availability of the services being migrated. This tool doesn't currently cover all aspects of a file and print server migration, but if you use ADS, AgileOne should be part of your arsenal because it vastly simplifies the management of hundreds of servers in any datacenter.

Dream Quest

None of the five tools tested fully supports the new file management concepts that are part of Windows 2003. Quest Consolidator seems to offer the most features for the price. It's the only one that provides comprehensive file usage analysis. So if you want to migrate both file servers and printers, this is the best tool to choose. Aelita Consolidation Manager performs all the operations supported by Quest Consolidator, but requires the Enterprise Directory Reporter to generate pre-migration reports. This makes it an expensive migration solution; in the end, this may be the reason why Quest has decided to move forward with Quest Consolidator after its purchase of Aelita.

Small Wonders Secure Copy also provides an easy solution for file migration, but would have to be combined with scripts to modify user settings as well as Microsoft's Print Migrator to support the migration of printers. PointDev's Ideal Migration is easy to use and works with most any Windows platform, but it may be over-kill if file and print server migration is all you need. It's also lacking in reporting capabilities. Consera AgileOne is a great tool, but its reliance on ADS makes it out of reach for many smaller shops.

If you want to take the simplest route to migrate your file and print servers, choose Quest Consolidator. It has its failings, but these will probably be addressed in later editions. M

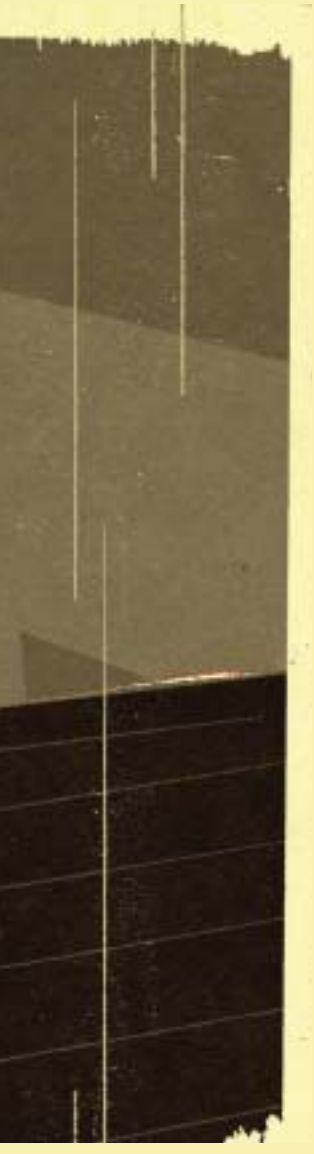
Danielle Ruest and Nelson Ruest, MCSE, MCT, focus on systems design, administration and management. They run a consulting company that concentrates on IT infrastructure architecture, and change and configuration management. Their latest book is Windows Server 2003: Best Practices for Enterprise Deployments. *Reach them at mcmag@reso-net.com.*

10 DNS Errors That Will Kill

DNS is the foundation the house of Active Directory is built upon. If DNS doesn't work, neither will your Windows network. Here are the 10 most common DNS errors—and how you can avoid them.

By Bill Boswell

Your Network



WELL OVER 70 PERCENT of all support calls that come to Microsoft support services that start out as Active Directory or Exchange calls end up being DNS calls. Yet, as you'll see in this article, most of these issues don't require extensive diagnostic work or sophisticated tools to isolate and resolve. I liken it to the days when automobiles had carburetors; a mechanic could fix most engine performance problems by fiddling with the choke—spritz a little WD-40 into the throttle body, charge $50 and retire in the suburbs after a few years. Nowadays, the same is true for DNS. Check the TCP/IP settings, run a few utilities to verify the zone records, charge $350 (correcting for inflation) and retire to Arizona.

You'll learn to identify the most common domain name system issues that cause problems for AD and Exchange and how to avoid them in the first place or isolate and resolve them if they occur in production. If you're an experienced Windows system engineer, they may seem a little trivial. But even the most highly trained and savvy administrator can get in a hurry and make a mistake. Also, the more experience you have, the more likely you are to make your DNS infrastructure complex, inviting the attention of Mr. Murphy and other elements of chaotic cosmic calamity.

1 TCP/IP Configuration Points to Public DNS Servers

This is by far the most common DNS error. Each network interface has a set of TCP/IP settings that lists the DNS servers used by that interface.

If the TCP/IP settings for a member computer specify the IP address of a public DNS server—perhaps at an ISP or DNS vendor or the company's public-facing name server—the TCP/IP resolver won't find Service Locator (SRV) records that advertise domain controller services, LDAP, Kerberos and Global Catalog. Without these records, a member computer can't authenticate and get the information it needs to operate in the domain. It then acts like a teenager who can't get the car keys, growing sullen and exhibiting a variety of bad behaviors.

Don't think this error can't happen to you. Let's say you're a VAR with a customer you plan to upgrade from NT 4.0 to Windows 2000 Server or Windows Server 2003. The desktops use DHCP with a scope option that includes the IP addresses of two DNS servers managed by the customer's broadband provider. The

Illustration by Elliott Golden

servers use static mappings to the same external DNS servers.

During the PDC upgrade, you install DNS because DCPromo tells you to. You let DCPromo configure a zone file that matches the DNS name you selected for AD. You're so pleased with the ease of the upgrade that you forget to reconfigure the TCP/IP settings of the newly upgraded DC to point at itself for DNS. You also forget to reconfigure the DHCP scope options so the clients still point at the ISP's DNS server instead of the new DC.

The result? The DC doesn't register SRV records in the new DNS zone and the clients wouldn't be able to find them, even if it did. The member computers don't know that the domain has been upgraded to AD unless they just happen to authenticate at the PDC. The other computers get no group policies, so you can forget about any carefully-orchestrated centralized management scheme. Your customer gets angry. You don't get a check for your services. Your children starve and your dog runs away. See the importance of DNS?

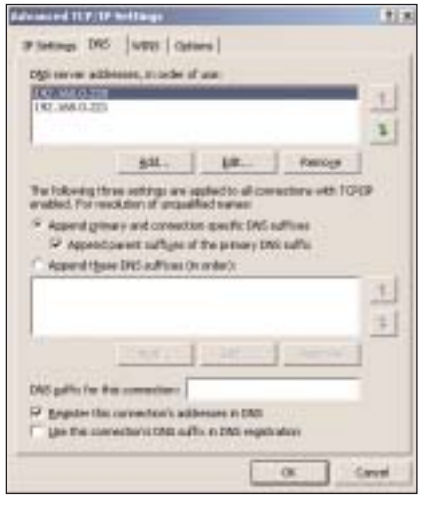


Figure 1. Advanced DNS properties for a network interface.

Fixing this problem couldn't be simpler. Once you enter the correct DNS entries in TCP/IP settings at the DC, populate the zone with SRV records by stopping and starting the Netlogon service. (If you've installed the Support Tools, you can run Netdiag /fix.) Now change the DHCP scope option to point clients at the new DC for DNS, then chase down any statically mapped servers and desktops and correct their DNS entries. Read the rest of the column for suggestions about resolving Internet names.

2 Improper DNS Suffix Handling

Users treat additional keystrokes as if they were penalties visited upon them by uncaring IT bureaucrats. Imagine what would happen if you asked your users to type Fully Qualified Domain Names (FQDNs) rather than simple flat names to connect to internal servers. *Quelle catastrophe*, as we say in southern New Mexico. Users are willing to type www.ebay.com to buy a used wristwatch, but they don't want to type \\w2k3s102.west.school.edu\freshman_zclass to map a drive.

DNS servers, however, stubbornly insist that every query specify a target domain. How else could they select the proper zone file? Simplicity vs. utility: It's a classic conundrum. The DNS resolver in Windows strikes a compromise. It accepts the flat name from the user then appends a suffix to form a FQDN it can send to a DNS server. The resolver obtains this DNS suffix from one of several places.

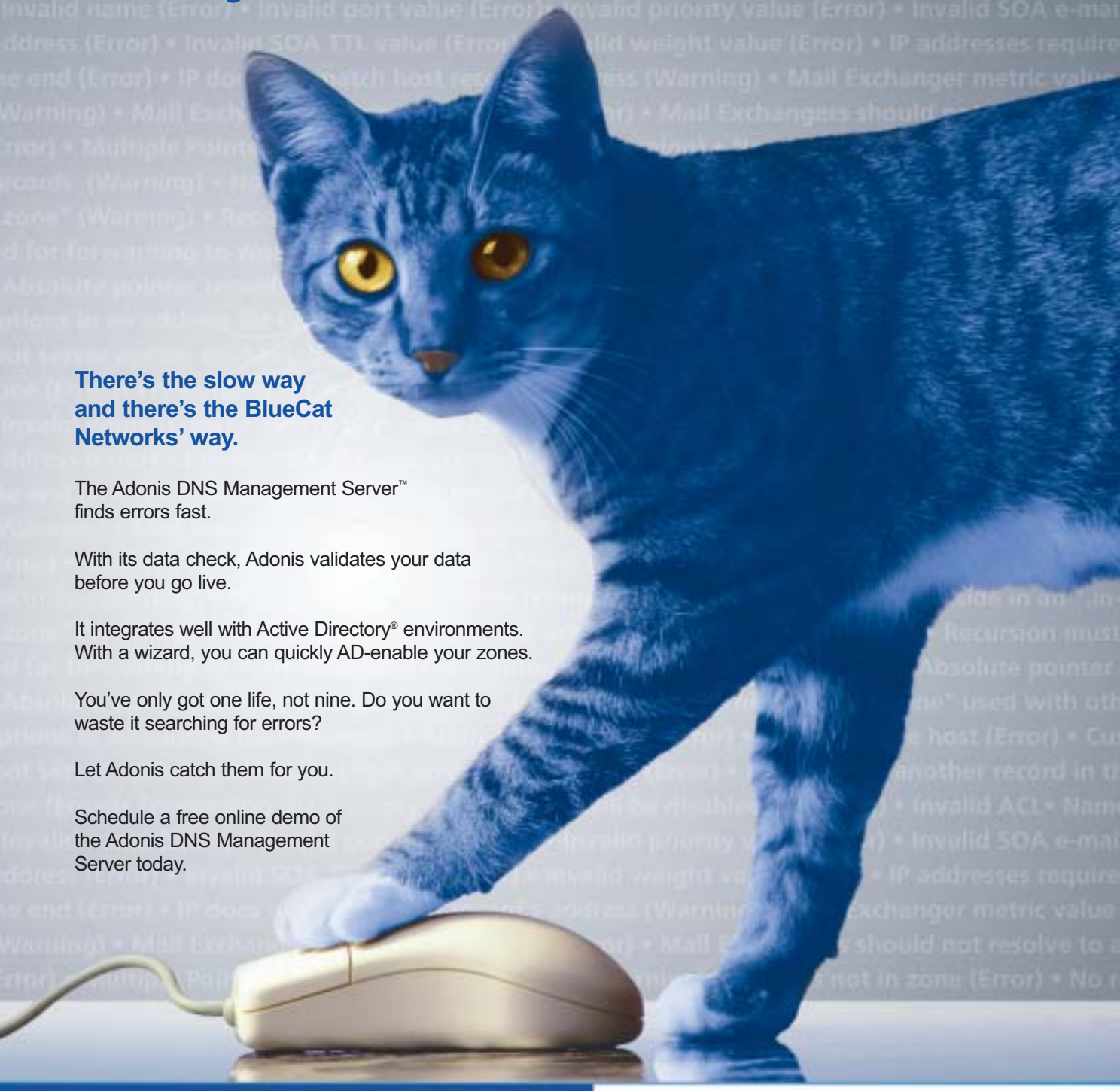
- *AD domain name.* The domain to which the desktop or server belongs has a DNS name as well as a flat name. You can see this suffix in the Properties of the local system (Figure 1). The TCP/IP Settings window calls this the Primary Suffix. If a query using the primary suffix fails, and the Append Parent Suffixes option is checked, the resolver strips the leftmost element from the primary suffix and tries again. For example, the resolver first appends west.school.edu then school.edu.
- *Interface suffix.* The TCP/IP settings for each network interface can have a unique DNS suffix, populated either statically or with DHCP. The user interface calls this the Connection-specific Suffix. It's best to leave this field empty in deference to the Primary Suffix. If you do give it a value, the resolver first tries the Primary Suffix, then the Connection-specific Suffix, then the parent suffixes of the Primary Suffix.
- *Search table.* The TCP/IP settings for all network interfaces share an optional set of DNS suffixes that the Registry calls a SearchList. If you elect to use the entries in a search list, the resolver ignores the primary suffix, its parents, and the connection-specific suffix.

In the default suffix search configuration, a client in the west.school.edu domain won't find a host in the east.school.edu domain. If you want a flat name to resolve to the host's actual FQDN regardless of the host's domain, select the Append These DNS Suffixes option and list each domain in the order you want them tested. Don't forget to include the FQDN of the local domain as the first option on the list.

3 Improperly Configured Forwarding

Ordinarily, when a client confronts its DNS server with a request for a resource record in an outside domain, the DNS server searches for a name server in the target domain and submits the query to that server. This standard query resolution has a couple of problems. First, the internal server can get so preoccupied chasing down recursive queries for public hosts that it runs out of resources to handle queries for its own zones. Worse still, the internal server must reach through the firewall and connect to a variety of DNS servers, some of which could have traps that play malicious games with DNS requests.

Can you catch **DNS ERRORS?**



There's the slow way and there's the BlueCat Networks' way.

The Adonis DNS Management Server™ finds errors fast.

With its data check, Adonis validates your data before you go live.

It integrates well with Active Directory® environments. With a wizard, you can quickly AD-enable your zones.

You've only got one life, not nine. Do you want to waste it searching for errors?

Let Adonis catch them for you.

Schedule a free online demo of the Adonis DNS Management Server today.

Visit www.bluecatnetworks.com or call 1-866-895-6931.

Network Computing Editor's Choice

Network Computing 2004 Winner

BLUECAT NETWORKS™

An internal root server doesn't need to waste energy or cause security problems by chasing referrals. Like a manager who doesn't want to get dirty hands, it can let some other DNS server do the grunt work. This process is called forwarding. The server that gets the job of doing the recursive queries and delivering the results is called a forwarder.

If you have a business relationship with an ISP, you might get an agreement with them to use their DNS servers as forwarders. This agreement would allow your DNS server to send recursive queries to the ISP's name servers. Otherwise, you can put a caching-only server in your perimeter network to use as a forwarder. If you have a public-facing DNS server in your DMZ that acts as the authoritative server for your public DNS domain, don't use it for a forwarder. Check out Error #7 to see why.

If you have a multi-tiered private DNS namespace supporting AD, configure the DNS servers in the child domains to use the internal root DNS servers as forwarders. This allows servers in the child domains to locate SRV and CNAME resource records in the root domain. Without these records, they can't replicate. Also, the root zone holds Global Catalog records for the entire forest. Exchange uses these records to find Global Catalog servers to use for message routing and group membership expansion. Outlook can be configured to find a local Global Catalog server from which to obtain the Global Address List.

Figure 2. The DNS zone properties showing the Start of Authority tab.

Don't forget to enable forwarding at each child DNS server. Do this even if you integrate the zone into AD. DNS servers store forwarding parameters in the local Registry, not in AD.

4 Improper Zone Transfer Configuration

In a standard text-based DNS zone, only the primary master DNS server has full Read/Write access to the zone file. Secondary DNS servers hold read-only replicas of the zone file. A resource record called Start of Authority (SOA) identifies the primary master server. Figure 2 shows the SOA properties.

Each change to the zone increments a serial number in the SOA record. Two zones in sync have matching SOA serial numbers. The primary master DNS server retains each zone change in a separate log file to use for iterative transfers. In iterative transfers, a secondary DNS server only pulls changes since the last zone transfer. The secondary servers keep track of zone changes using the SOA serial number.

It's not uncommon for DNS administrators with BIND experience to make changes directly to a zone file. This can cause zone transfer issues with Windows DNS because not all updates reside in the main zone file. It's usually a good idea to stick with the graphical interface or use a command-line tool such as Dnscmd to make changes to a zone.

Windows DNS servers use TCP rather than UDP for a zone transfers, so if you have an intervening firewall, be sure it allows TCP connections over port 53. Also, Windows DNS servers don't use Port 53 as the source port for zone transfers. So when configuring a firewall, expect packets in the zone transfer to come from any port above 1023.

Don't allow unrestricted zone transfers. Configure the zone to allow transfers only to servers whose name appears in the Name Server list, as shown in Figure 3. The Name Server list doesn't get populated automatically. Manually add the FQDN and IP address of each secondary server. By placing a secondary server on the Name Server list, you also enable the primary master to send notifications of changes to the secondary server. It's worth the trouble. Disable zone transfers completely at secondary servers unless you want another secondary to pull the zone from it.

Before you make the switch to using AD-integrated zones, remove secondary zones from any DCs. If you forget to do this, you put the DC in the awkward position of getting a replica via standard zone transfers and a copy in AD. Remove the secondary zone then stop and restart DNS to see the AD-integrated zone.

Test zone transfers using a tool called *dig* that comes with the BIND implementation from the Internet

Illustration by Elliott Golden

A practical security solution for businesses from 10 to 100,000 employees.

Millions of patches quietly managed. Thousands of potential threats averted. And counting. If you want to keep your workstations and servers safe, but don't want to spend hours doing it, let Shavlik HFNetChkPro handle the patching. It's the industry standard patch management tool that automatically scans and pushes patches across your network, so you can concentrate on other matters. And, hit the road home early for a change.

To download our Free version, visit www.shavlik.com, call (800) 690-6911 or email us at info@shavlik.com.

Secure Your Vision.

Shavlik

Systems Consortium (ISC). The most current version of BIND (and dig) is 9.2.3. Get the Win32 binaries from www.isc.org.

```
dig @w2k3-dc1.school.edu school.edu ifxr=87
; <<>> DiG 9.2.3 <<>> @192.168.0.250 school.edu ixfr=89
;; global options:  printcmd
www.school.edu.   3600   IN     CNAME   webserver2.school.edu.
school.edu.       3600   IN     SOA     w2k3-dc1.school.edu. hostmaster.school.edu. 90 900 600 86400 3600
```

Listing 1. The dig syntax to transfer the last name change iteratively.

Using dig, you can initiate full or incremental zone transfers and see the results. For example, to test an incremental transfer, first query for the SOA record at the primary master to see the current serial number. Then request an iterative transfer (IXFR) specifying an earlier SOA serial number. For example, if the SOA serial number is 88, the dig syntax to do an iterative transfer of the last zone change would be similar to the code shown in Listing 1.

This listing shows the SOA and a CNAME record called www.school.com that points at a server named webserver2.school.edu.

Figure 3. DNS Zone properties, showing the Name Server list with authorized secondary DNS servers.

5 Failure to Verify Dynamic Update of Resource Records

Every modern Windows client periodically registers its A and PTR record with the Start of Authority (SOA) server for the forward and reverse lookup zones, respectively. The clients send their record updates to the SOA servers because, in standard BIND-style DNS, only the SOA has a Read/Write copy of the zone file. In AD-integrated zones, any DC running DNS can update a zone record.

The DHCPClient service on a Windows computer handles the dynamic updates for each network interface. Don't disable this service on a statically mapped server; you'll prevent the server from updating its DNS records if you (or a colleague, after you're long gone) change the server name or its IP address.

DCs use the Netlogon service to register their SRV records along with the CNAME records that contain each DC's Globally Unique Identifier (GUID.) These CNAME records are vital for replication. To assure accurate entries, the Netlogon service updates DNS hourly using the content of a file called Netlogon.dns, located in %windir%\system32\config.

The SRV and CNAME records have a format that determines the record's location in the DNS hierarchy within the zone. This hierarchy is important because domain members query for SRV records at specific locations. If these lookups fail, the machine gives up and uses local logon credentials.

Invalid or missing SRV records can also cause problems for Exchange 2000 and Exchange Server 2003. Modern Exchange relies on DCs to store information about the Exchange organization, and uses the Global Catalog extensively to support messaging routing and to help down-level Outlook clients expand the membership distribution lists. By the same token, newer Outlook clients can be configured to use local Global Catalog servers to obtain address lists, so they rely on DNS as well.

A fast way to check for proper SRV record registration is to use the Netdiag utility that comes in Support Tools. Netdiag performs a suite of checks, but here's the syntax to perform just the DNS test with verbose output saved to a Netdiag.log file:

```
netdiag /v /l /test:dns
```

This test walks through every entry in the Netlogon.dns file and verifies that the server has all the proper DNS entries. If you have multiple DCs, you'll get a minor error because the DNS query results in all DCs, but the overall result will come up as a PASS if all the results match.

If you get a FAIL on the Netdiag test, use the log file to determine the problem record. You can use Netdiag /fix to apply the contents of the Netlogon.dns file to DNS again. If this resolves the problem and it doesn't reoccur, then all's well. If the problem happens again, you'll have to do more digging.

One particularly aggravating source of SRV record problems isn't a lack of records but too many records. If you have a DC with multiple interfaces, the default action of DHCPClient is to register each of the interfaces. If one of the interfaces connects to a private network, such as a dedicated backup network, then clients will fail when they get that IP address, forcing them to go back to DNS to get another SRV record and slowing down the logon process. This can also happen if you have a management card in the server that presents its network or modem interface as a standard network connection which DHCPClient insists on registering.

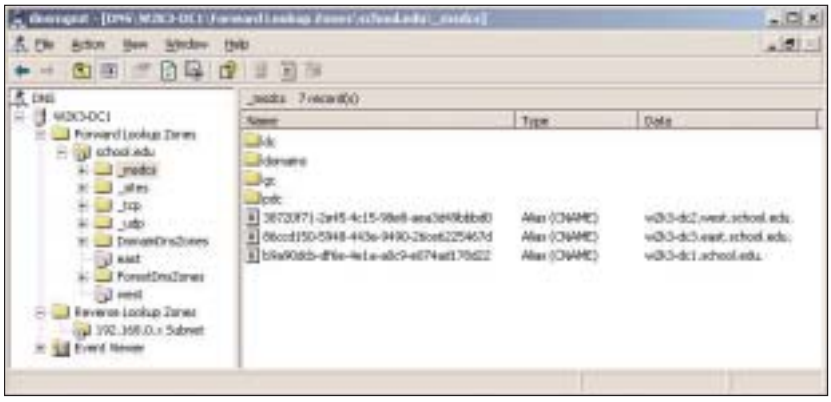


Figure 4. The DNS management console showing CNAME records for DCs in an AD forest.

6 Failure to Properly Delegate Child Zones

All DCs in a forest share a common copy of the Configuration and Schema naming contexts, so DCs need to find replication partners regardless of their domain. AD identifies domains and DCs in DNS using CNAME records that correlate a server's GUID and its FQDN. Figure 4 shows the list of CNAME records for the School.edu forest.

If a CNAME record references a server in a child domain, the root DNS server needs to go to a DNS server in the child domain to retrieve a copy of the server's A record. It gets the name of this DNS server by way of delegation.

In delegation, the parent zone contains NS records that specify the names of DNS servers in the child domains along with A (glue) records that contain their IP addresses. Win2K and Windows 2003 use a New Delegation Wizard to create these records. The wizard walks you through selecting the child domain name and identifying name servers in the child domain.

If someone takes down a child DNS server for maintenance, or decommissions it entirely, without notifying the DNS administrator in the parent domain, the delegation records in the parent zone become invalid. This is called lame delegation. You can also get lame delegations by blocking zone transfers to a secondary server if the secondary server has an NS record in the parent zone. This sometimes happens during an overzealous security sweep.

In an AD forest, lame delegations can cause replication failures as the

root DNS servers grope for the IP addresses of the DCs in the child domains. You'll get Event Log entries complaining about RPC (Remote Procedure Call) connection errors and the inability of the Knowledge Consistency Checker to get a complete spanning tree topology. Lame delegations can also cause connection failures when desktops in one domain try to connect to servers in other domains, although this might not be obvious right away if you use WINS.

If you deploy Windows 2003 DNS servers, you can avoid lame delegations by using stub zones. This feature creates a small zone file on the parent DNS server populated with copies of the SOA, NS, and A records from the child zone. The parent DNS server periodically refreshes the stub zone contents, drastically reducing the chance of having a lame delegation.

Figure 5. DNS Server properties showing the option to avoid using recursion when forwarding.

My favorite tool for diagnosing delegation problems is the DNSLint utility from Microsoft. You can download DNSLint from download.microsoft.com/download/win2000srv/Utility/Q321045/NT5XP/EN-US/dnslint.exe.

DNSLint is a command-line utility that does two sets of tests: one to determine if your DNS configuration supports a specified AD domain, and one to determine if your DNS configuration meets standard practices for a zone. For example, DNSLint determines the name servers for a zone then checks that each server responds to a request at UDP Port 53 and that each server has matching, valid SOA records and NS records. It also checks for valid MX (Mail eXchange) records that point to e-mail servers in the target DNS domain.

7 Failure to Secure Public-Facing DNS Servers

For security, you want all internal servers to rely solely on forwarders to resolve Internet names. Don't let your internal servers roam the Internet looking for name servers. Select the "Do not use recursion for this domain" option when configuring forwarding. Figure 5 shows an example. This essentially makes your internal DNS server a slave of its forwarders; so specify two or more forwarders and try to use servers in different subnets, if possible. You don't want a network failure at your ISP to keep your clients from resolving DNS names.

Now let's turn attention to the servers you'll use as forwarders. It's important to keep the two primary DNS functions—caching and zone table lookups—on separate servers. If you allow your primary public DNS server to accept recursive queries and cache the results, you open yourself up for cache pollution. That's why you want to install a caching-only server in your DMZ to act as a forwarder, rather than using your public DNS server as a forwarder.

For example, let's say your DNS server gets a recursive query for www.deviousdomain.com. It finds the name server for deviousdomain.com and asks for the www host record. In return, it gets the host record but it also gets a flock of name server (NS) records for domains such as Microsoft.com, Yahoo.com and so on, along with glue records that have IP addresses pointing at nefarious Web sites. Check the option to Disable Recursion for all public-facing authoritative DNS servers.

You should also enable cache pollution filtering in the DNS server Advanced properties. Do this for any server that accepts recursive queries, internally or externally. Cache pollution filtering tells DNS not to cache NS and glue records for domains outside the authoritative zone of the name server that sent them and not to cache glue records for the responding server's authoritative zone, just in case a bogus name server impersonates the actual server.

Block all traffic to public-facing DNS servers except for UDP port 53. On the private side of the DMZ, you'll need to open TCP Port 53 and all ports above 1023 to permit zone transfers between multiple DNS servers in the perimeter network. You can protect this traffic using IPSec if your firewall accepts IPSec traffic.

For public-facing servers, take a look at the advice in RFC 2870, Root Name Server Operational Requirements. Some of the restrictions apply only to the gTLD server operators, but the suggestions and requirements for maintaining a secure, safe DNS platform are worth your consideration. Also, take a trip to www.dnsreport.com to get a great quick-and-dirty analysis of whether your public-facing DNS servers exhibit common DNS problems.

8 Failure To Properly Secure Resource Records

If you use a BIND-style primary master to store a zone, you shouldn't allow

dynamic updates. Windows can't secure updates to a text-based zone file. Any machine can assert itself as an existing host and overwrite the A record with a new IP address. This essentially allows a machine to hijack the DNS records of another machine.

If you want to use dynamic updates for a zone, integrate the zone into AD and permit secure updates only. This requires a client to use Kerberos to validate its identity, then initiate a secure transaction to obtain a signing key that it can use to digitally sign the update request. RFC 2930, "Secret Key Establishment for DNS," documents this method, which can only be used by modern Windows clients (Win2K, Windows XP and Windows 2003).

Other DNS servers support secure dynamic updates, but not using this method. Examples include the current version of BIND, Lucent VitalQIP and Incognito's DNS Commander. These servers use a form of DNS security that requires a shared secret key. Windows clients don't support shared secret keys. For more information about DNS Security (DNSSEC), read the RFCs listed at www.dnssec.org/rfc.php.

9 Incorrect, Outdated or Unreachable DNS Servers

Anyone can get in a hurry and type an incorrect IP address in a host record or misspell a server name in a CNAME record. DNS doesn't validate your entries—it assumes you're a consummate IT professional and accepts your input unquestioningly. For this reason, it's a good idea to test every new entry you make into a zone. If you do this as a habit, the test becomes a reflex.

The best test of a new A or CNAME record is usually a quick ping right at the console of the DNS server or your workstation. Take a couple of precautions to keep from getting fooled by caching. Both the DNS server and the local DNS resolver cache any records they receive for a period of time determined by a TTL setting in the record. The SOA for the zone determines the default TTL, which is one hour for Windows DNS servers. Clear the local cache using ipconfig /flushdns. For the server, use the Clear Cache option in the server's property menu in the DNS console or use the Dnscmd utility with the syntax dnscmd <server_name>/clearcache.

Typos aren't the only source of misinformation in DNS. You can get interesting problems if you remove a member server from service but forget to remove the corresponding A and PTR entries from DNS. Or you might remember to remove the A record but forget to look for any CNAME records that reference the A record. This can be difficult to troubleshoot if you reference multiple servers with the same host name. Windows DNS uses round robin load sharing; so if you take a server down for maintenance and forget to remove the A record from DNS, not every client gets an invalid A record. Windows DNS also uses round robin for cached entries, so flush the cache if you take a DNS server down for maintenance.

» Your customer gets angry. You don't get a check for your services. Your children starve and your dog runs away. See the importance of DNS?

You also get invalid DNS entries if you use AD-integrated zones and demote a DC that was also a DNS server. The server still has DNS running, but has no local zones so it starts acting as a caching-only server. Depending on the forwarding configuration and NS records stored in the local Registry, it might even appear to work normally, which is unfortunate. It would be better if it failed completely so you could fix it right away.

Clients can also get invalid information if you set up a public-facing DNS server behind a NAT firewall and the server has glue records that reference private IP addresses. A typical NAT firewall doesn't translate the IP address in glue records, so the DNS server passes out referrals to servers that can't be touched from outside the firewall. You should avoid publishing private addresses entirely or get an application layer gateway capable of translating glue records.

» Don't let your internal servers roam the Internet looking for name servers.

10 Lack of Fault Tolerance

As systems administrators, we're trained to think about the possibility of server failures and operational flexibilities. You would probably not set up a single DNS server in a large enterprise because your entire computing operation would grind to a halt if you take the server down for maintenance. But would you put the second DNS server on the same rack as the first? Or in the same subnet? Or even in the same server room?

Fault tolerance is all about assessing business risks, and if your business relies heavily on DNS, it makes sense to put some thought into maintaining continuity of service. You'll get a big head start by integrating your DNS zones into AD. This allows you to use any DC in the domain as a primary master DNS server, eliminating the single point of failure in standard BIND-style DNS. Also, because each DC represents itself as the SOA server for the zone, its DNS clients do their dynamic updates locally rather than sending them across the WAN to a single primary master.

If you do decide to use a standard text-based zone, decide in advance which secondary server you'll promote in the event of a failure of the primary master or a loss of the network connections to the primary master. Scheduling maintenance can be tricky, because you don't know when a client will attempt a dynamic update, but as long as you have secondary servers, the clients won't lose the ability to do read-only queries. However, a zone with a Windows SOA expires after 24 hours, so don't dilly-dally with getting the primary master back on line.

If your organization covers a large chunk of planetary geography, you may want to consider putting the _msdcs portion of the root domain into its own zone and putting a secondary of that zone on all your DNS servers. This allows DCs to find the CNAME records of their replication partners without querying across the WAN.

If you use AD-integrated zones, a common question arises about where to point the DCs themselves for DNS lookups. For the most part, you can point a DC at itself and specify an alternate DNS server in the same site.

There's an exception to this rule. In the forest root domain, don't point the DCs at themselves. The CNAME records in the _msdcs portion of the forest root zone identify the DCs in the forest. You can end up in a Catch-22 situation where a forest root DC can't find the CNAME record for a replication partner and can't get a copy of the CNAME record because it can't replicate. Windows Server 2003 resolves this problem by automatically going to another DNS server if it can't find the CNAME record corresponding to a DC GUID in AD.

Don't Forget the People

All of the problems and errors listed in this article can be avoided by planning and testing. There's a final problem, though, that transcends technology. It's a people issue.

In many organizations, the need to support AD in DNS puts the Windows folks in the same meeting room with the Unix folks who control the existing DNS servers. Sometimes those meetings achieve spectacular results. The participants use their long history of mutual trust to share insights into their own needs and requirements and, in doing so, they create a design that incorporates all the best features of Windows DNS and BIND or VitalQIP or DNS Commander, or whatever flavor of DNS is running on the Unix servers.

Other times, the results of the meetings aren't quite so collegial.

As you work for a compromise that allows you to mix different versions of DNS in the same organization, keep these words of Doug Floyd from Spokane's *The Spokesman-Review* in mind: "You don't get harmony if everyone sings the same note." M

Contributing Editor Bill Boswell, MCSE, is an independent consultant, trainer and founder of The Windows Consulting Group. He's the author of Inside Windows 2000 Server *and* Inside Windows Server 2003, *as well as* Inside Exchange Server *(Addison-Wesley). Contact him at bboswell@winconsultants.com.*

IBM Express Middleware: Designed and developed for midsize companies.

(IBM muscle for less moolah.)

MIDDLEWARE IS POWERFUL IBM SOFTWARE. The kind of software that makes your applications work better to solve your business problems. It's an answer. It's IBM DB2,® Lotus,® Tivoli® and WebSphere.® And in the form of the IBM Middleware Express Portfolio, it's now more accessible than ever for midsize businesses.

The IBM Middleware Express Portfolio is engineered to work with your existing business applications whether they run on Windows,® Linux® or UNIX.® It's engineered to be deployed by those without computer science degrees. It's priced to put a smile on Accounting's face. It's nimble. Quick. Flexible.

Your technology will work harder to meet the demands of your customers, your business goals and your industry's needs. It makes your business more responsive to the unforeseen. Of course, all of this is easy to implement, easy to install, simple to maintain. You need to learn more. To find an IBM Business Partner in your area, visit **ibm.com**/software/express

IBM


Spending valuable time manually tracking assets?
Facing a sudden hardware or software upgrade?
Frustrated by the limitations of your Help Desk?
You have
BETTER
things to do!
With Alloy Software's
premier software solutions,
IT managers
can now easily:
Establish effective IT infrastructure management
Perform automated hardware and software audit
Verify software license compliance
Facilitate fast problem resolutions
Maintain comprehensive knowledge base
Prepare for hardware transitions and software upgrades
Alloy Software
Free Extended Evaluation License
To order, call Alloy at 201.656.0404
or email to sales@alloy-software.com
use promotion code MPC1103
www.alloy-software.com, phone: 201.656.0404, fax: 201.656.9988

By Joe McKendrick,
ENTmag.com

Special to *MCP Magazine*

Windows Server 2003 Gains Traction

THE WINDOWS SERVER 2003 ROLLOUT IS RAPID, ACCORDING TO A NEW SURVEY. KEY DRIVERS ARE SECURITY, ACTIVE DIRECTORY AND EXCHANGE 2003.

GROWING REQUIREMENTS around security, Active Directory and Exchange Server are propelling widespread adoption of Windows Server 2003, according to a new joint survey of ENTmag.com and Microsoft Certified Professional Magazine readers. Six out of 10 Windows sites are already in some stage of rolling out Microsoft's latest server operating system.

But most Windows Server 2003 migrations are focused on practical front-end or departmental functions in the enterprise, such as Web serving, e-mail and file/print services. Only a limited segment of companies plan to deploy high-end enterprise applications such as ERP or data warehouses on Windows 2003. And only a handful of organizations are considering moving to 64-bit versions of the operating system. Also notable is the scant consideration being given to enhancing Web services capabilities. Despite the enormous industry attention being devoted to Web services, Microsoft's .NET Framework isn't even a blip on the radar screen for many IT shops making or considering the move to Windows 2003.

ENTMAG.COM
To read the full results of this survey, go to www.entmag.com/reports/article.asp?EditorialsID=61

The survey covers a range of companies and industries from mainly across North America and finds rapid adoption of the new OS taking place.

Most Windows shops are now in the process of moving at least some applications to Windows Server 2003.

The survey of 163 IT managers and executives confirms that 60 percent of Windows sites either already have Windows 2003 in production or plan to do so very soon. As shown in Table 1, one in six companies currently has the OS in production, and 43 percent have migrations in progress.

Another 20 percent of Windows shops aren't ready to commit to a timeline for Windows 2003, but say they'll deploy the new OS on a case-by-case basis as older applications are replaced. The survey also finds that among the 20 percent of companies that don't have any plans to migrate, more than a third say it's because they've just completed a migration to Windows 2000.

Once the migration process is under-way, respondents plan to ramp up to Windows 2003 fairly quickly across their enterprises. Currently, 63 percent of companies in the survey report that more than half their servers are running Win2K. Within a year, a majority, 52 percent, expect to be running Windows 2003 on most of the servers across their enterprises.

Most enterprises are moving to Windows Server 2003 for

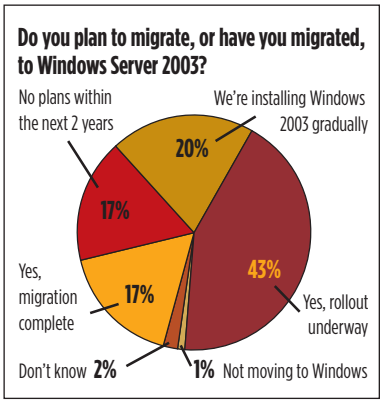


Table 1. Migration plans.

new security, e-mail and Active Directory features.

In an era of rampant viruses, worms and hacking incidents, security is driving many migration efforts to Windows 2003. Windows platforms and applications have been a highly publicized target for malicious code writers, bringing Microsoft considerable pressure to deliver more secure systems and a more manageable approach to patches and updates.

In the survey, security is cited as one of the top three leading reasons for migrating to Windows 2003, with almost one-sixth of the group, 16 percent, calling it the primary driver for moving to Windows 2003 (see Table 3). A large majority, 77 percent, cite security as a secondary reason for deploying Windows 2003.

Active Directory, a key component of the Windows 2003 security infrastructure, was another key factor cited in migration plans. About one out of six respondents, 17 percent, indicate they're moving to Windows 2003 to take advantage of Microsoft's directory services (Table 4), while 37 percent cite this as a secondary reason.

The need to upgrade to Exchange Server 2003 is also driving many migration plans, the survey finds. About 16 percent cite this as their main reason for moving, while a majority, 59 percent, list it as a secondary reason.

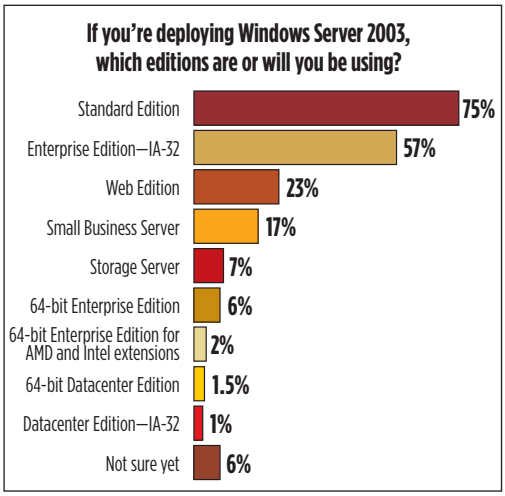


Table 2. Windows Server 2003 editions.

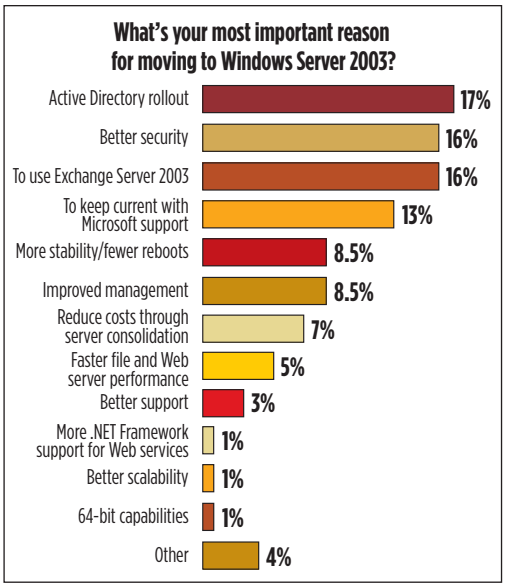


Table 3. The top reasons for moving to Windows Server 2003.

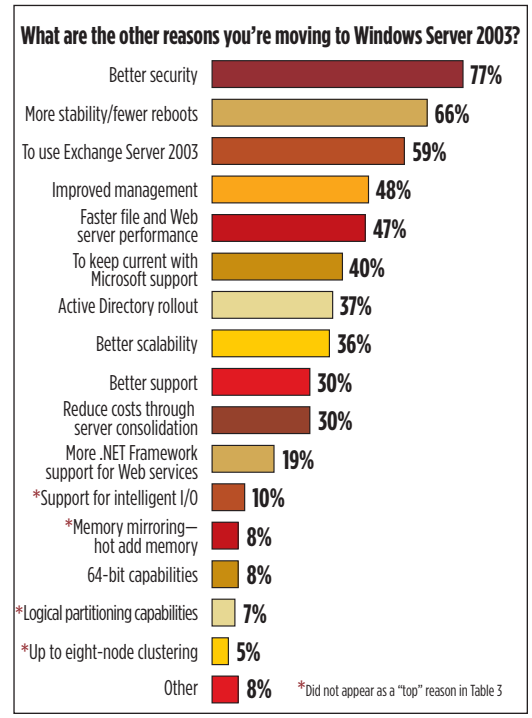


Table 4. Secondary reasons for moving to Windows 2003 Server.

Alleviating the reboot problems endemic with prior versions of Windows is driving many upgrade plans as well. More than eight percent say this is the single most important reason, and two-thirds cite this as a secondary reason. At least one respondent, however, cautions that Windows 2003 isn't entirely free of these problems. "Windows Server 2003 still appears to have memory and thread management problems," said the IT manager at a large financial services company. "We still have to reboot our Windows Server 2003 servers periodically, particularly after deploying security patches."

Ranking surprisingly low in the list of priorities in migrating to Windows 2003 is the desire to more effectively implement Microsoft's .NET Framework-based Web services. Microsoft has positioned .NET as the cornerstone of its enterprise strategy going forward, but it appears more practical operational issues are driving Windows OS migrations. Only one company cited .NET as a primary reason for moving to the newer OS, and only 19 percent rank this feature as a secondary driver.

Other enterprise-class attributes—including logical partitioning, clustering and scalability —rank low on the priority list and only surface as secondary reasons.

Windows Server 2003 will mainly be deployed for tried-and-true Windows-style applications.

To a large extent, Windows 2003 will be picking up the mantle of applications first deployed in Windows NT and carried forward to Win2K. Large majorities of respondents expect to be deploying such tried-and-true Windows functions as file-and-print functions, e-mail, and Web servers. A majority, 53 percent, also report they'll be deploying Windows 2003 to support transactional databases. M

Joe McKendrick is an independent consultant and author specializing in surveys, technology research and white papers. Reach him at joe@mckendrickresearch.com.

THE POWER TO SEE.

ELM Enterprise Manager 3.1 gives you the power to see the health and status of your systems at a single glance. Imagine the time savings and productivity increases available when event frequencies, performance trends, state changes, and quality of service breaches are clearly displayed and easily accessible.

ELM Enterprise Manager benefits:

- **Saves Time**
- **Rapid ROI**
- **Secure**
- **Reliable**
- **Available**
- **Affordable**

Equally important, be alerted by email, page, or instant message when it is time to take a quick look. Get a critical head start on problem identification and resolution with ELM Enterprise Manager.

To experience how real time monitoring will benefit you, visit www.tntsoftware.com and

DOWNLOAD YOUR FREE 30-DAY EVALUATION COPY TODAY

ELM ENTERPRISE MANAGER

How the First-to-Know Stay Ahead.™

Certified for Microsoft® Windows Server™ 2003 Standard Edition Enterprise Edition Datacenter Edition

Certified For Microsoft Windows Windows 2000 Advanced Server Windows 2000 Server

Microsoft® GOLD CERTIFIED Partner

TNT Software

www.TNTSoftware.com

To speak with a representative, call 360.546.0878 (8-5 PST)
or e-mail sales@tntsoftware.com

YOUR RIDE TO SUCCESS

JOIN THE $300 BILLION COMPUTER SERVICE BUSINESS.

Find out how you can invest in one of *Entrepreneur Magazine's* **"HOT 100 Franchises"**, and in a *Franchise Times* **"FAST 55"** company.

Single, Multi-Units and Area Development Opportunities are now available.
For more information call

888-667-4577
(ext. 307)

or visit us at:
geeksoncall.com

GEEKS on call®

Readers Review Exchange Server 2003

By Doug Barney, Reviews Editor

IN AN ENTIRELY NEW APPROACH TO PRODUCT REVIEWS, 13 LOYAL **MCP MAGAZINE** READERS DETAIL THEIR EXPERIENCES RUNNING EXCHANGE 2003 IN PRODUCTION ENVIRONMENTS.

PRODUCT REVIEWS TEND to follow the same mold—bring in some hardware or software, set it up in a lab and have someone pound on it until they decide if it's any good. There's nothing wrong with this approach, but for the complex and feature-laden Exchange Server 2003, we thought there was a better way.

That's why *MCP Magazine* literally broke the product review mold. We created a framework, or set of evaluation criteria, and then interviewed over a dozen readers who shared their real-world experiences. These were all IT professionals running Exchange 2003 in a production environment.

So Many Servers, So Little Time

Microsoft claims that if you shell out the dough for a bunch of Exchange 2003 licenses, you'll actually save money. And if you architect your network properly, the company is absolutely right.

The biggest area of saving—and headache reduction—is through server consolidation, made possible two ways. Windows Server 2003 offers the ability to do more with each server, especially when compared to NT. Exchange 2003 (and 2000) adds to that the ability to have more than one database (mailbox store) per server. With Exchange 2003, database size is realistically only limited by hardware (with a 16TB upper limit). There can be up to four storage groups and 20 databases per server.

Some users contacted by *MCP Magazine* back the Microsoft claims. "Together with a domain consolidation (13 NT 4.0 domains, single master domain model consolidated to one single Active Directory domain based on Windows 2003), we've been able to limit the number of Exchange mailbox servers to three cluster servers. In the existing environment, based on Exchange 5.5, we used 11 mailbox servers, including four cluster servers (not including servers for dedicated purposes like bridgehead, IMC, etc.). The limited number of Exchange servers will greatly reduce efforts needed for maintenance, including patching, backup, etc. compared to the old infrastructure," said Patrick Egloff, IT systems engineer working for a large travel company in Switzerland.

Battling Bandwidth

The Outlook client, when working with Exchange 2003 (Outlook 2000 still works with the new Exchange), has improved caching, so there are fewer requests to the server and, thus, less traffic across the network. On the other side, Exchange has more efficient compression, so these same messages are smaller in terms of pure bytes than with previous systems. The MAPI compression has been found to reduce traffic by as much as 70 percent for Pacific Life, according to a case study posted on www. microsoft.com.

The combo means there's less pressure on IT to regularly boost LAN or even WAN bandwidth. "In our new environment, we use Outlook 2003 in Exchange Cached Mode, [with a] full install on every client. The users seem to be very happy with the new solution, as they no longer experience delays during typing, printing and logon. In addition, we have been able to successfully reduce the traffic used for messaging on the small WAN links," said Egloff.

Illustration by Neal Aspinall

Security 101 for Exchange 2003

Microsoft gets mixed security reviews from customers. "[Outlook Web Access] S/MIME integration was an absolute no-brainer. We were already using digital certificates and had public keys integrated into Active Directory, so installing the S/MIME control was the only thing we had to do to enable Signing/Encryption capabilities. Additionally, we store the certificates on USB security key fobs and no additional configuration was necessary. This was very well implemented, a major upgrade," said Sean Wallbridge, principal consultant/trainer for itgroove limited, a professional services firm in British Columbia.

Not all are so easily impressed. "Security has been enhanced, but I don't think drastically. One other improvement that is nice is the ability to implement blocking lists. I have done this on just about every deployment. Obviously, it isn't a total solution to [unsolicited commercial e-mail], but it helps," said John LeClair, senior systems engineer for Compuquip Technologies, a Florida IT consulting firm.

Security is a problem Microsoft should never stop working on. "I had a lot of issues with being a relay server. I couldn't find a balance between allowing my Web servers to relay, but no one else's. It's not as easy as Microsoft documents make it sound. In a standalone environment it's very secure," said Brian Gibson, systems administrator for the UK-based The Q Group, which makes software for the education market.

Storage and Backup Shine

While Microsoft brags about Exchange's dramatic new storage features, a close look reveals that most of these attributes come from Windows 2003 itself, such as Volume Shadow Copy Service (VSS).

"One particularly nice feature is the integration of Exchange 2003 with the Volume Shadow Copy Service of Windows 2003, which allows for huge time saving during backup restores," said Egloff. "Being able to use [VSS] for Exchange backup is nice, as it allows for backups in almost no time. We decided to use this technology vs. a dedicated, third-party backup agent. We back up the databases via VSS to a local disk and transfer this backup file to our centralized backup solution. Doing so we no longer have to pay for expensive agents (if available at all) and can use all the official backup and restore guidelines from Microsoft," he added.

Exchange May Never Crash Again

Say the word "Windows" to anyone running older software, and they'll likely cringe at the memories of crash after crash. And more recent software isn't immune from the occasional lapse into inoperability. But Exchange 2003 is a far cry from the flaky days of Windows 95, NT 4.0 and the very first release of Exchange.

For instance, improved virtual memory technology reduces the fragmentation that used to regularly bring down earlier Microsoft messaging platforms. And that means the darn thing doesn't crash so much. "At one point the [Exchange 2003] server had been up for five months, still not having a reboot after installing Exchange and the anti-virus management console—without a single problem, memory leak or any slowdowns at all. I see no reason that a Windows 2003/Exchange 2003 server would ever have to be rebooted under normal operating conditions," said Eric Phillips, network consultant for LTI Information Technology, a Michigan technology firm.

Faster Than a Speeding Exchange 2000

IT pros are like sports car nuts—always after the speed. In the case of Exchange 2003, Microsoft delivers. While the improved virtual memory reduces crashes, it's also designed to increase performance by making variable memory requests rather than swapping fixed values and turns many small memory requests into larger, more efficient blocks.

The result is snappier software. "On the same hardware, Windows 2003/Exchange 2003 appeared to perform about 30-percent faster and booted 200 percent faster," said itgroove's Wallbridge.

The Web client also satisfies sub-millisecond speed junkies. "OWA performance improvements were noticeable immediately. Trimming of variables, etc. all led to much better performance, even over slow links," said Wallbridge. M

Read the Full Report

IT folks are a savvy lot, and a non-supported platform can be kept running with the occasional application of duct tape. So even for frugal Exchange 5.5 users, Microsoft has to make the new Exchange compelling enough to switch to and stave off the lure of e-mail platforms from other vendors.

We went to the best source we could find—*MCP Magazine* readers—to see if the Microsoft hype stands up to real user scrutiny.

The full report, from which this article is excerpted, documents reader experiences with Exchange 2003 ROI, bandwidth, performance, server consolidation, mobile access, RPC over HTTP, security, anti-spam functionality, Outlook 2003 and Outlook Web Access, and more. Download your copy at http://mcpmag.com/resources/exchange_reviewed/

Your life shouldn't.

The new iHateSpam Server Edition lets you control spam according to the needs of your company and users—not to mention *your* needs. ***Spam detection easily better than 90%—right out of the box:*** You can "configure it and forget it" for easy, effective "hands-off" spam management. Set up takes minutes, not hours or days. ***Low false positives:*** Control aggressiveness of spam detection with simple threshold settings. Set server or user-level whitelists. And end-users always get email from the people in their own Contacts folder. ***Constantly updated spam engine:*** Field-tested, powerful spam detection engine. ***Filtering based on tunable parameters:*** Use our default engine or customize with your own rules or blacklists. ***Customizable treatment of spam:*** Delete it, route it to a designated mailbox, put a custom message in the subject, or even quarantine it to a spam folder in the end-user's mailbox. ***Filter at the server—no client software needed:*** Set flexible server-level policies for large groups or single users.

Windows & .NET MAGAZINE Readers' Choice 2003
WINNER
Best New Product
Best Antispam Tool

iHateSpam Server Edition
for Microsoft Exchange 5.5, 2000 and 2003

SUNBELT SOFTWARE

SPECIAL OFFER: Try a FREE demo and get a "SPAM SUCKS" mug: www.sunbelt-software.com/ihse

Sunbelt Software Tel: 1-888-NTUTILS (688-8457) or 1-727-562-0101 Fax: 1-727-562-5199 www.sunbelt-software.com sales@sunbelt-software.com

Thin Clients, Fat Heads

By Kevin Kohut

THIS BUSINESS OWNER'S THIN-CLIENT WINDOWS NETWORK WAS IMPREGNABLE. OR SO HE THOUGHT, UNTIL HE MET BOB...

I GET A CALL from one of my customers. "There's something wrong with the network. Everything is really slow." I tell him I'll look into it right away. As I start to check it out, I get a call from another client.

"We're really crawling here. Is there something wrong?" I tell her that we're already checking it out, and we should have things back to normal soon.

Another client, then another, calls, each with the same complaint. One more comes in. This time my customer offers an explanation: "I think there's a virus on the network!"

VIRUS? NO WAY!

A virus? There's no way we could have a virus. Yes, this was all happening in the midst of a serious virus outbreak, and yes, many large corporations had already been infected, but not our systems. Let me explain.

My company, EasyOffice Network (EON), provides clients with comprehensive, thin-client–based, fully-managed IT solutions. We supply, build, configure, manage and retain ownership of all computer systems used by our clients. I've built most of these IT infrastructures from the ground up and have employed best practices in how we manage everything from desktop machines to file severs to routers to firewalls. I've been doing this for a long time and am proud of a long track record of keeping my clients' systems in good working order.

We're able to do this thanks to several key elements of our service model:

- The capabilities of Terminal Services in a Windows 2000/XP environment.
- The licensing agreement we have with Microsoft that allows us to rent the use of Microsoft software to our clients.
- The ability to remotely administer the computers and network systems in place at our client sites.
- The fact that our high-end data center systems are used to support several clients.
- The proprietary expertise we incorporate into our system configurations.

Because we use a server-based computing model with thin-client workstations, the technical requirements for one of our IT solutions are quite different than those for a traditional office network environment. To illustrate, let's look at a typical EON solution.

Our customer, Little Guy Industries (LGI), has two locations: their main office in Los Angeles and a smaller branch office in San Jose. We put a file server, an application server, a SQL server and a domain controller in the Los Angeles office. In San Jose, we placed a domain controller (which also serves as a file server) and an application server. The application servers run Terminal Services. All servers are configured with real-time virus-checking software.

THIN IS IN

For the clients, we use LGI's existing Dell computers—a mixture of older Celeron- and Pentium III-based machines. We rebuild all the Dells with a standard Windows XP Professional configuration. These machines are used to do one thing, and one thing only: run the Remote Desktop Client to connect to an application server. They won't be used for Internet brows-

Illustration by Peter Bennett

ing; they can't even get out to the Internet! As such, we don't install any kind of virus scanning software on clients—remember, all program activity takes place on the application server through a terminal services session; nothing actually takes place on the client machine.

The offices are each connected to the Internet via DSL, protected by industry-standard firewall appliances. Interoffice network communication is handled by a hardware-based VPN. Only the servers have access to the Internet, and then only through a firewall.

Now that you have an idea about the typical EON environment, let's see what happens when trouble's afoot. Suppose it's a Tuesday morning, and word of a new virus threat makes the rounds. One of our standard procedures is to check the firewall traffic logs to see what kind of packets are hitting our networks from the outside, and sure enough, we find evidence of attempted attacks. We contact our upstream Internet provider (if they haven't already contacted us first) and ask them to keep tabs on the traffic going through their networks.

We also check our server logs for evidence of virus activity. They show lots of attempts but no infections. Thanks to the faithful real-time virus scanning software installed on each server, no one suffers any ill effects from this attack.

We've survived one of the more destructive and widespread virus attacks that have come down the pike in a long time. Feeling ever so smug in our prowess over infectious bytes, we send an e-mail to all our clients detailing how severe this virus attack was to many Fortune 500 corporations—and emphasizing how not one of our clients suffered even as much as a sniffle.

Virus Outbreak No. 2

Several weeks later, another virus outbreak. We dutifully carry out our standard procedures, and again our servers are undaunted. We're thinking about sending out another boastful e-mail—but wait! Our clients start reporting problems—slow performance, unable to connect, dropped terminal server sessions.

OK, so we hold off on sending the "We beat the virus" e-mail to our customers and start troubleshooting. Could these problems be related to the virus outbreak? No, we think, just an untimely coincidence. There's got to be something we can find to explain these problems.

After observing heavier than normal network traffic, we find that there is, indeed, evidence of virus activity on our internal networks. So I ask my techs to pore through the firewall logs again. But this time, I tell them to look at activity from inside our NAT-compliant, firewall-protected, private networks. "But the only way into our private networks is through public Internet gateways, and we've already proven that nothing came through any of our firewalls," my senior tech points out.

I repeat my instructions. He begrudgingly complies with my request. Later that day I get an e-mail from my tech. He tells me that he was able to narrow down where all this virus mayhem began—at one of our client sites (let's refer to this client as "Bob"), from inside the private network. As I'm contemplating how this could have happened—how a virus could just appear in a private network without any trace of it coming through the firewall—I get another e-mail. This one is from Bob.

He tells me that he thinks his laptop is infected with a virus and wants to know what to do about it. "What laptop?" I think to myself. We never sold or discussed a laptop computer with this client. I e-mail him back. I tell him how to discover the MAC address of his NIC and give this bit of information.

I pass this info on to my tech, and he confirms that Bob's laptop is the source of all this extra network traffic. Further analysis reveals that none of our other internal subnets started having problems until after Bob's laptop started doing its thing.

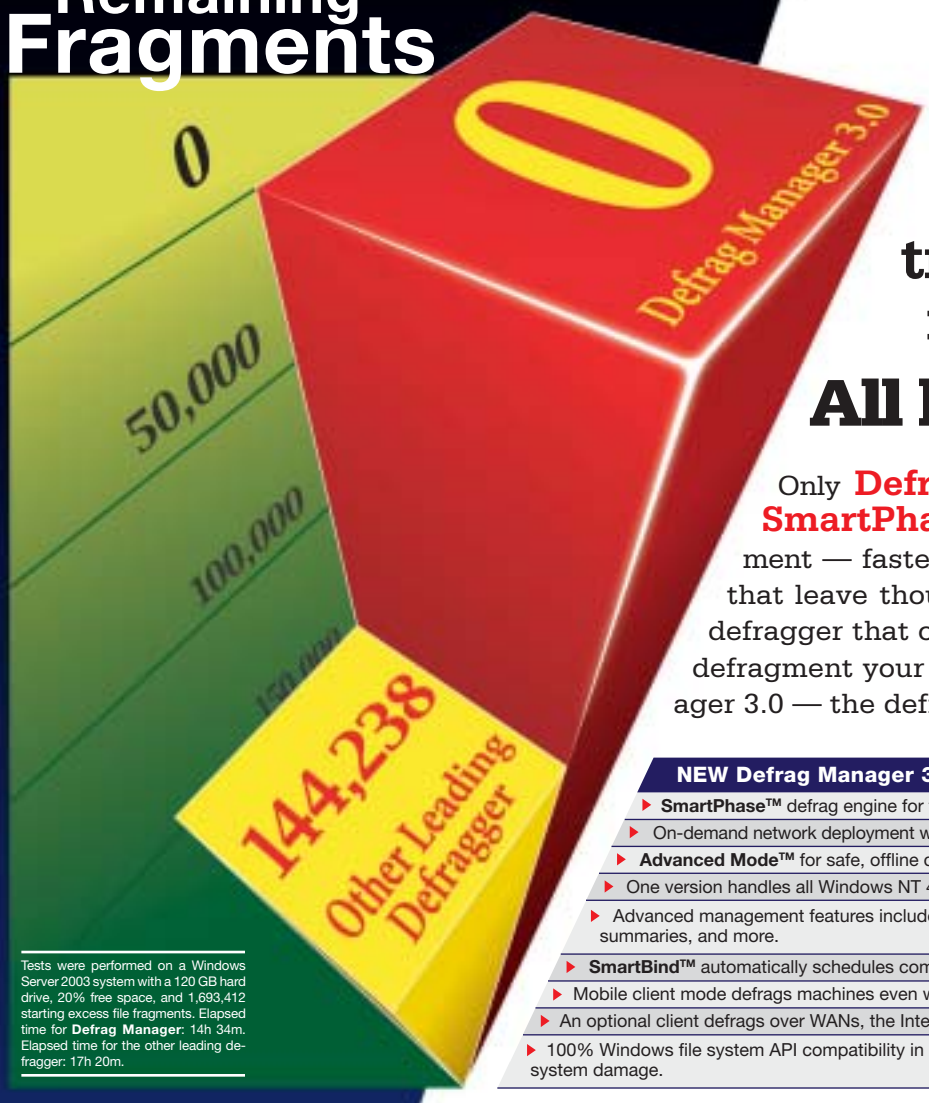
Virus? Way!

Sure enough, all our virus issues started with Bob's laptop. He brought it into the office, plugged it into the network, and that was it. Our servers were undaunted. They were used to being

Secure Your Thin-Client Network

Securing a thin client network is similar to securing a traditional network. You want to protect network systems from outside attack, inside attack, and system failures. Here are three tips specific to thin client-based networks:

1. It's all about the servers. Not only do you need to protect the servers from viruses, hardware failure and so on, you also need to protect them from the users themselves. If a user hoses his or her Office installation in a traditional network environment, you have one computer (and one user) down; in a thin-client environment, a hosed Office install puts everyone out of commission.
2. Tame Internet Explorer! Running IE through a remote desktop session can open up your application server to hundreds, if not thousands, of security issues. Spyware, toolbars, popups, and all those other Internet annoyances can cripple a terminal server. Either tightly lock down IE on the server, or let your users browse locally.
3. Group Policy is your friend. Proper use of group policies, including the "User Group Policy loopback processing mode" policy, found in the Computer Configuration | Administrative Templates | System | Group Policy container, will make the job of securing terminal servers a whole lot easier.



Tests were performed on a Windows Server 2003 system with a 120 GB hard drive, 20% free space, and 1,693,412 starting excess file fragments. Elapsed time for **Defrag Manager**: 14h 34m. Elapsed time for the other leading defragger: 17h 20m.

NEW 3.0

Every defragger tries for zero fragments.

All but one fail.

Only **Defrag Manager™ 3.0** with **SmartPhase™** can remove every fragment — faster than competing products that leave thousands behind. Why buy a defragger that only *attempts* to completely defragment your systems? Get Defrag Manager 3.0 — the defragmenter that succeeds.

NEW Defrag Manager 3.0 features:

- **SmartPhase™** defrag engine for faster, more thorough performance.
- On-demand network deployment without end-user interaction or third-party tools.
- **Advanced Mode™** for safe, offline defragging of all files, folders, and metadata.
- One version handles all Windows NT 4.0, 2000, XP, and Server 2003 machines.
- Advanced management features include drag-and-drop scheduling, real-time summaries, and more.
- **SmartBind™** automatically schedules computers as they're added to the network.
- Mobile client mode defrags machines even when they're disconnected.
- An optional client defrags over WANs, the Internet, and non-NetBIOS networks.
- 100% Windows file system API compatibility in all modes of operation eliminates potential file system damage.

Repair. Recover. Accelerate.

Learn More!
1-800-408-8415
www.winternals.com

Winternals®

buffeted with attacks. But our thin-client workstations? They were never designed to be in a hostile environment. Their only purpose in life is to connect with a Remote Desktop Connection to a Terminal Server, all inside a private network.

OK, so we needed to get these thin-client machines working properly again. And we needed to do this in a way that minimized downtime. Thankfully, this was pretty easy. Remember, all the applications used by our customers are run from terminal servers, and all their data files are stored on servers, as well. Because the thin clients didn't have anything installed on them other than the operating system and remote desktop clients, all we had to do was re-image them, a 10-minute process using our disk imaging software.

But, even at only 10 minutes a pop, with dozens of machines to re-image in disparate locations, it still took the better part of a day to complete the task. No data was lost, and our clients suffered little actual downtime.

Lessons Learned

But Bob's little laptop adventure did make us think about revamping our security procedures—and our contracts. From now on, we'll be stricter in enforcing our policies and making sure our clients are held accountable for following them.

For starters, we reworked our standard contract to include specific language about our customers' responsibilities regarding their own equipment. But anyone who's in this line of work knows that a contract is only good after the fact. Because our goal is to have satisfied clients, we also revamped our thin-client image to include anti-virus software. Yes, it costs us more; but, hey, our customers are worth it.

We're also examining more sophisticated technology solutions to address this area, specifically in the areas of DHCP and network switching. If we can prevent a non-EON client device from getting a valid IP address in the first place, we've pretty much nipped the problem in the bud. Again, this increases costs, and at some point we'll have to pass them on to the client.

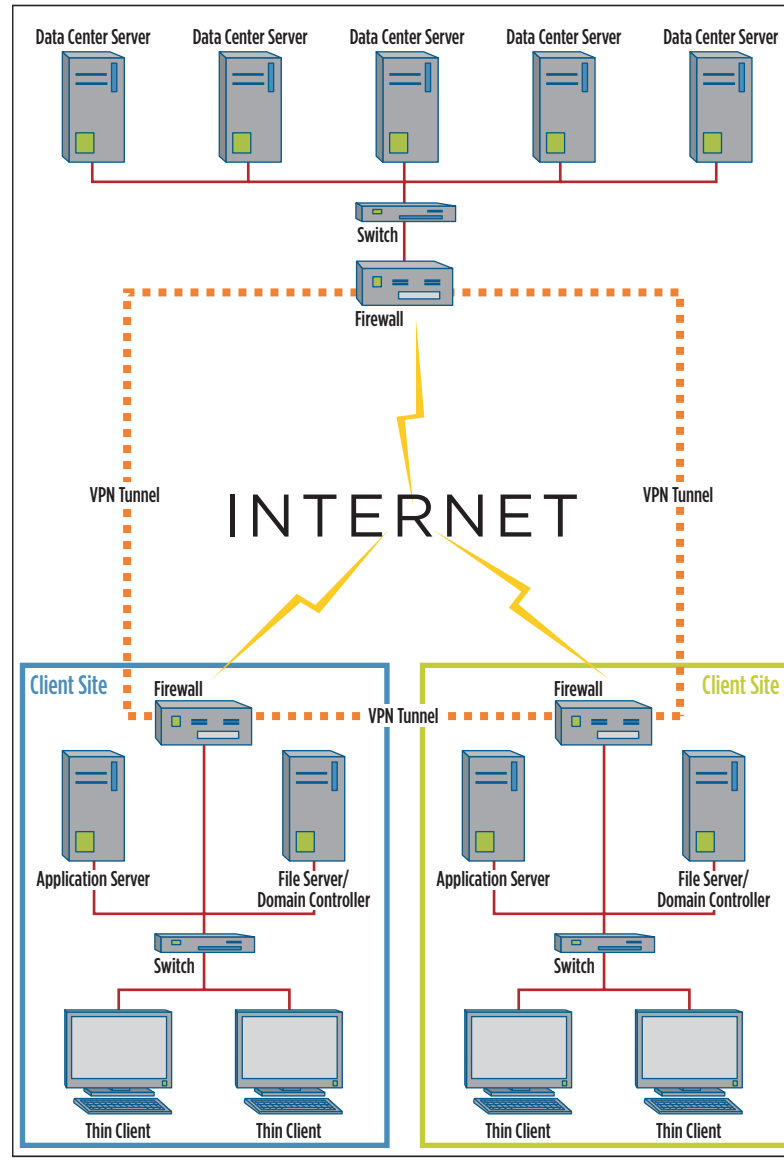


Figure 1. A typical EasyOffice Network thin-client arrangement.

Are You Ready for Bob?

"OK Kevin," you may ask, "nice story and all, but what does this have to do with me?" Well, if you're an IT pro responsible for maintaining computer systems (or even if you're not), realize that you can't just rely on technology to keep things running smoothly. This latest wave of viruses may not have caused you or your users any trouble, but eventually you're going to have deal with a Bob of your own. And all the anti-virus software in the world won't protect you. Are you ready for Bob? M

Kevin Kohut has been involved with information technology in some form or another for over 18 years, and has a strong business management background as well. As a computer consultant, Kevin has helped both small businesses and large corporations realize the benefits of applying technology to their business needs. Drop him a line at kk@easyofficenetwork.com.

EMC²
where information lives

10 Reasons to Choose EMC for Your Exchange 2003 Infrastructure

1. Exchange 2003 enables significant site consolidation. EMC expertise in data center consolidation can help you gain maximum financial benefit from your upgrade.

2. Microsoft recommends SAN storage for Exchange 2003. EMC is the world leader in storage area network technology and utilizes jointly-developed, Microsoft-endorsed best practices to implement state-of-the-art storage solutions for your Exchange environment.

3. As your e-mail becomes more and more mission-critical, you should be talking to a world leader in business continuity and disaster recovery solutions: EMC.

4. Microsoft uses EMC storage and software in its own Exchange 2003 environment, as well as in a number of development labs around its Redmond campus.

5. EMC knows how to manage large-scale data migrations. EMC has performed more data center migrations and consolidations than any other vendor.

6. EMC and its LEGATO division are world leaders in information lifecycle management and experts in today's compliance and regulatory minefield. EMC offers complete archiving and compliance services and solutions to safeguard your intellectual property and achieve regulatory compliance from e-mail creation to archival.

7. EMC's tiered storage approach lets you optimize your infrastructure and choose the storage solution that best fits your environment—from high-performance data center arrays to ATA-based online archiving systems—throughout the lifecycle of your Exchange information.

8. Every EMC Proven™ Exchange Solution is fully tested and backed by a complete portfolio of Microsoft Exchange-related services to help you plan, design, implement, and manage your Exchange environment.

9. EMC does significant engineering and joint development with Microsoft, has contributed to many significant Windows-oriented storage initiatives, and was first to support many of Microsoft's new storage APIs, including Volume ShadowCopy Services.

10. EMC offers the industry's most highly rated post-sale service and support to make sure your mission-critical e-mail environment is up and running around the clock.

For more information, go to www.EMC.com/microsoftsolutions.

Analyzing Your Baseline Security

A couple of years ago, Microsoft offered a free utility called HFNetChk. Written by Shavlik Technologies (www.shavlik.com) and licensed to Microsoft, this utility included an XML database of security issues and updates and could be used to scan Windows computers for potential security problems. Shavlik sold (and still sells) HFNetChk Pro, a graphical version of the utility.

Today, Microsoft has replaced HFNetChk with a friendly, graphical tool called the Microsoft Baseline Security Analyzer (MBSA). That's a subtle name: It's not a complete security analysis, but it does say what minimum stuff your servers are missing in order to have a shot at being considered secure. MBSA can be downloaded free from www.microsoft.com/mbsa. The current version, 1.2, scans for security problems not only in Windows but also in SQL Server, Exchange, MDAC, MSXML, BizTalk, Commerce Server, Content Management Server and Host Integration Server—all remotely, if you like. For local scans, MBSA can even find security issues with Microsoft Office. It also checks the configuration of the Internet Connection Firewall, Automatic Updates client, IE zones, the MBSA tool itself and more. It's an awesome utility with a robust command-line interface that lends itself especially well to automation.

For example, say you want to scan a remote server and get a report of missing security updates, improper configurations and so forth. Nothing could be simpler! Just run:

```
mbsacli.exe /c domainname\computer-
name
```

Even better, scan every computer in an entire domain by using:

```
mbsacli.exe /d domainname
```

Or, if your servers are in a block of IP addresses, scan them with:

```
mbsacli.exe /r aaa.aaa.aaa.aaa bbb.bbb.
bbb.bbb
```

specifying the appropriate IP addresses to define the start and end of the block containing your servers. If you have an SUS server on your network, specify the /sus server option and MBSA will only report on updates that you've approved for distribution through SUS and will ignore unapproved updates. Want your security report to go to a file? Add the /o filename parameter and specify an output path and filename. For best effect, run something like:

```
mbsacli.exe /d domainname /o filename
```

once a month using the Task Scheduler, and you'll have a monthly report of security issues on every computer in your domain—a perfect To Do list for the intern who's starting next week!

The cool part about MBSA is that it's more than just a list of updates you need to install; the Automatic Updates client could take care of that. MBSA also lists configuration issues that aren't corrected by an update, such as a SQL Server computer with a blank password for the all-powerful "sa" account. You'll be tipped off to these configuration problems and can fix them for an immediate boost to your network's security.

Batch Files Still Usable

If you're one of the proud, few admins who has used HFNetChk, all of your batch files aren't useless. Run MBSA with the /hf command-line parameter and it'll accept HFNetChk command-line parameters. That means your HFNetChk batch files can be easily ported to use MBSA: Just search and replace "hfnetchk.exe" with "mbsacli.exe /hf" in your .bat files.

Contributing Editor Don Jones, MCSE, is a founding partner of BrainCore.Net and a popular trainer, speaker and author. His latest books are Managing Windows with VBScript and WMI *(Addison-Wesley) and* IIS 6.0: Step-by-Step Mega-Guide *(CertCities.com). He's at donj@braincore.net.*

"A world-class vulnerability scanner that won't make a hole in your budget."

Laura DiDio
Senior Analyst, Yankee Group

Close the door on hackers.™

You can't close the door if you don't know which one is open. That's why we designed Sunbelt Network Security Inspector (SNSI): **A low-cost, quick-install, fast-result vulnerability scanner** that uses a top quality, commercial-grade database of ranked vulnerabilities. **Prioritized vulnerability reports** provide detailed and easy-to-follow instructions on how to fix holes fast, so you can focus on the most critical security issues. **Configurable scans**—create your own scans or use predefined scans such as "high risk" or the "SANS top 20." **Windows platform support:** Find holes in Windows 95/98/ME/NT/2000/XP and Windows Server 2003 machines. **The easy, all-new interface** has a short learning curve—just point, right-click and scan.

Network Security Inspector™

SNSI is licensed per Administrator and lets you scan unlimited machines! SNSI won't make a hole in your budget, so you can afford to be proactive without compromises.

$949 per Admin* Unlimited Machines!

SPECIAL OFFER: Install a FREE demo and get your own black "Hack My Network and Die" T-shirt. Check out the offer and download the demo at www.sunbelt-software.com/snsi.

SUNBELT SOFTWARE

Sunbelt Software Tel: 1-888-NTUTILS (688-8457) or 1-727-562-0101 Fax: 1-727-562-5199 www.sunbelt-software.com sales@sunbelt-software.com

*Competitive upgrade price. Yearly maintenance (25%) not included. Upgrade from *any* currently available vulnerability scanner. *Even freeware!* Regular price: $1,495. See www.sunbelt-software.com/snsi for details.

DANIELLE AND NELSON RUEST

STEP-BY-STEP

Install Help Files from Other Operating Systems

One of the greatest features of Windows Server 2003 is all the information available for it. And while the information found on the Microsoft Web site and elsewhere on the Web gives a lot of details, in the end it serves more as a starting point than anything else.

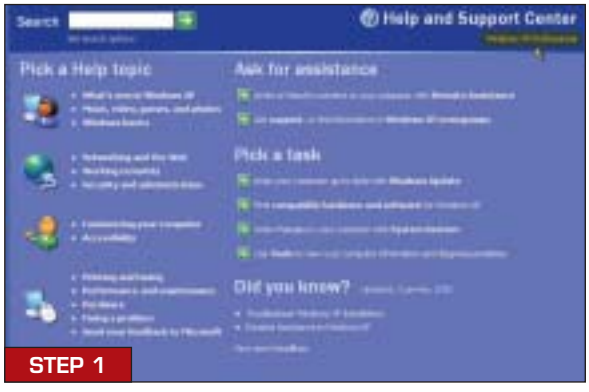
Whether you're working on the architecture phase of your Windows 2003 deployment or you've already deployed it and are now administrating it, you'll want to have Windows Server 2003 information "at your fingertips," so to speak. One of the best ways to do this is to install the Help files from the operating system locally on your PC. This option is available only on Windows XP and the Windows 2003 family, because it makes use of XP's new Help and Support engine.

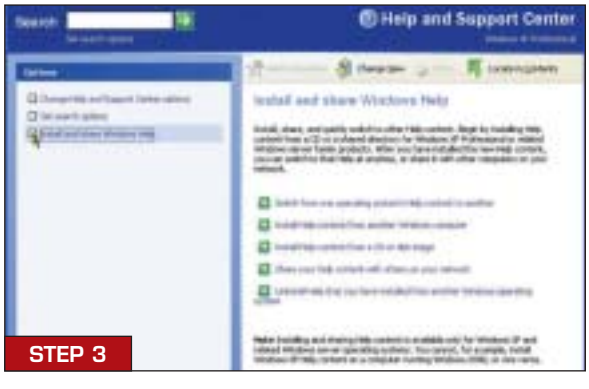
You can install Help content from different versions of the Windows Server 2003 family—Web, Standard and Enterprise—so that you can search for information on each directly from your PC. Once installed, you can switch from one OS's help system to any other. While each edition includes much of the information contained in the others, you may want to install all the ones you're working with because of the particularities of each specific edition. At the very least, the minimum you should install is Windows Server 2003, Enterprise Edition, because it offers the most comprehensive content. Here's how to proceed.

STEP 1: Use Start Menu | Help and Support to launch the Windows XP Help and Support engine. Note the help version you're using in the top right corner, in this case, Windows XP Professional.

STEP 2: In the Help and Support toolbar, click Options in the top right portion of the window. A new menu appears in the left pane of Help and Support window.

STEP 3: Click Install and share Windows Help in the left window pane. This displays the installation and sharing





options in the right window pane. These options let you switch from one Help system's content to another, install Help from another computer, from CD or from a disk image, share Help with others on the network, or uninstall previously installed Help content.

STEP 4: Now, click Install Help content from a CD or disk image. Once again, the right window pane contents will change. Insert the Windows 2003 Installation CD from which you want to copy the help files.

Note that the Autorun feature of your CD drive will cause the Windows 2003 installation splash screen to open; simply click Exit to close this screen and continue with the procedure.

Type the drive letter of your CD in the drive listing or click Browse to locate it, then click Find once you've returned to the Help and Support window. Help and Support will read the CD and list the available Help contents in the bottom of the right window pane.

STEP 5: Select the Help you want to install from the list in the bottom right window pane, then, click Install. Help and Support will perform the installation. Once finished, it will list the new Help as being Already Installed. You can repeat steps four and five if you want to install more than one OS' Help content.

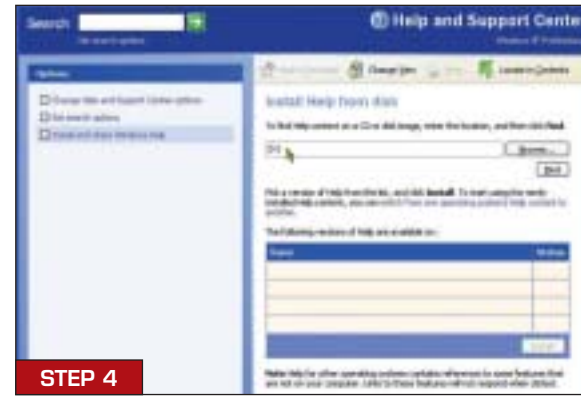
STEPS 6 AND 7: Click Switch from one operating system's Help content to another in the middle of the right window pane. Select the OS you need, then click Switch. Help and Support will open the Help content you requested. Note that it lists the name of the new Help system in the top right corner of the Help and Support Center window.

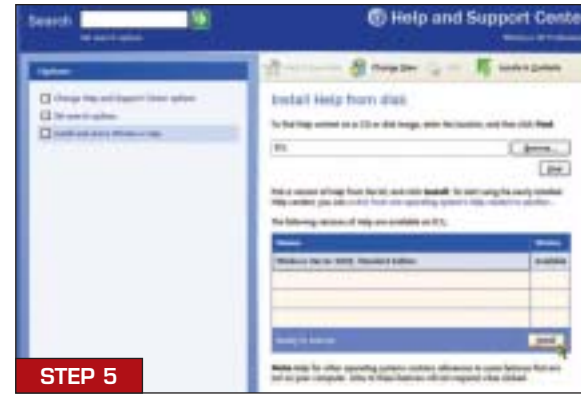
From now on, when you want to switch from one Help Content system to another, launch Help and Support, click Options and select Switch from one operating system's help content to another, select the OS required and click Switch.

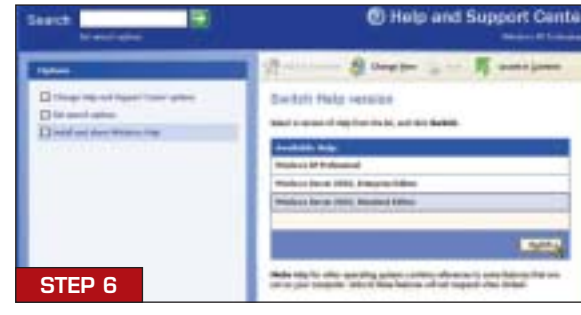
This gives you access to valuable information on all aspects of the Windows 2003 operating system. Finally, you'll truly have "information at your fingertips." M

If you'd like to see a particular procedure explained step-by-step, send e-mail to Editor Keith Ward at keith.ward@mcpmag.com. Put "Step-by-Step" in the subject line.

Danielle Ruest and Nelson Ruest, MCSE, MCT, are book authors focusing on systems design, administration and management. They run a small consulting company that concentrates on IT infrastructure architecture and change and configuration management. You can reach them at mcpmag@reso-net.com.







ROBERTA BRAGG SECURITY ADVISOR

The Hidden Risks of Process Controls

What are the most powerful networks in the world? Those that run the government offices of powerful nations? Those that connect the offices, employees, customers and suppliers of Fortune 500 companies or international commercial ventures? Banking networks? The CIA? FBI?

The most powerful networks in the world aren't data networks—they're process control networks, which control the operation of devices. They may be heating and cooling (HVAC); building security; factory machinery; water supply; power grids; phone networks. A sample listing of what process control networks handle would include:

MCPMAG.COM
The online version of this article includes the threat model created by NIST and the Process Control Security Requirements Forum.

- Pumping air in a building.
- Controlling lighting during surgery.
- Controlling locks on office doors.
- Regulating flow of oil and gas.
- Handling manufacture of paper and power.
- Controlling traffic lights and systems of major cities.
- Regulating the seat-belt warning, ABS and engine management systems on your car.

Some day they'll control nearly every critical and non-critical function where automated controls can be used. These control networks may have just a couple of nodes, or potentially millions of them.

So what should we be doing to prevent some evil genius or a 14-year-old with a twisted sense of coolness from disrupting essential services, endangering lives or playing Russian roulette with the building controls of our offices?

THE BASICS

In my house, an automated thermostat controls the operation of my heating and air conditioning. I use a simple wall-mounted device to program desired temperatures, time of day and days of the week. Sensors detect room temperature and actuators, directed by a simple decision-making computation, turn heat or air conditioning on or off to maintain temperatures. It's convenient and hasn't needed repairs or adjustments. HVAC systems that control larger buildings and other process control systems that manage the operation of manufacturing, mining and core infrastructure systems are, of course, more complex. Still, the same principles are in effect. Sensors provide information used in decision-making. Actuators make changes in response to automated or directed control decisions. A human interface system is provided for operations, monitoring and maintenance. Unlike my simple system, however, most process control systems are part of control networks.

Control networks use standard protocols to communicate over different types of media. Older process control networks used proprietary protocols over RS-232 and RS-485 serial communications networks. The decision-making or control devices were also proprietary and programmed using proprietary languages. Remote maintenance was either not performed or primarily accomplished over dial-up. These networks didn't interface with data networks.

Today's process control systems often run on Windows NT or XP and are connected to data networks. Device control mechanisms (those simple, inscrutable black boxes that are physically close to or part of the actual physical system and may monitor and make adjustments on their own) may also still be proprietary, but are accessible to administration stations over TCP/IP networks via gateways that convert and filter communications. Furthermore, many devices now include the capability to use IP as the transport mechanism for serial communications or are directly accessible using TCP/IP to permit control and reporting functions.

The rationale behind using the data network to provide control of process control systems is classic. It reduces cost; increases the ability for distributed control; eliminates a single point of failure for monitoring; enables better, more efficient, more coordinated control and monitoring of distributed mechanisms; and increases the distance over which control can be performed. (Many off-

shore drilling rigs, for example, are now unattended. They're controlled via radio communications from remote land-based administration centers.)

SCADA AND DCS

Different types of control networks exist. You may have heard about supervisory control and data acquisition (SCADA) networks. These networks are used to control the operation of critical infrastructure services. SCADA systems are typically managed over a local LAN, although they may be connected with other SCADA systems via satellite, leased line, PSTN or Internet. Another type of control network is DCS, or distributed control system. These networks typically locate main administrative functions in one place, but control distributed devices at remote locations. The figure below illustrates a sample network.

NOT DESIGNED WITH SECURITY IN MIND

Like data networks, control networks were originally developed for business and convenience reasons. They were developed with little consideration for security or with primary security considerations being physical. They were conceived by people whose expertise is in the process side, not the IT side.

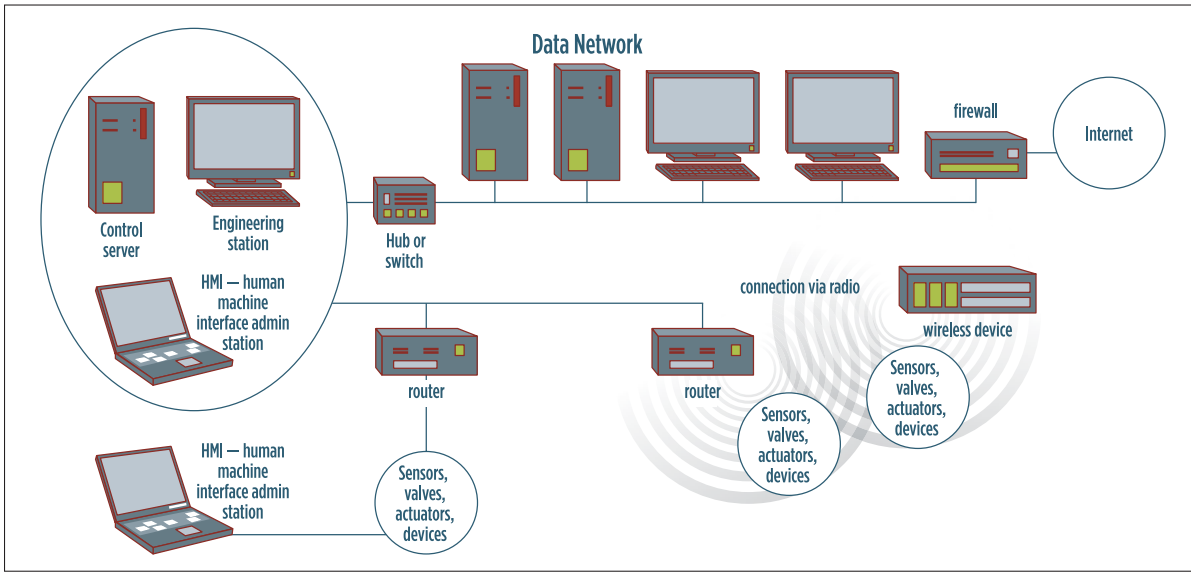
Security for the majority of devices in operation today is non-existent or turned off. Like data systems, process control devices and applications are generally shipped with security functions disabled to make installation easier. Because installers may not be properly trained, and organizations may lack any knowledge of security requirements, security features may not be implemented or will continue to run with defaults still set. On many devices, security consists of the ability to password-protect access. IT personnel are at a distinct disadvantage, as they may not recognize the security issues. The use of the data network as a transport for control networks doesn't appear to offer any increased threat for the IT network, and the technologies used in control operations are foreign to most IT employees.

When the individuals who should be most concerned with the secure operation of these devices—process control engineers and IT systems administrators—are not only not aware of the risks, but have no basis for extended communications, and their management shares their naiveté, it's only a matter of time before accidental or malicious use of these networks results in disruption of services or, at worst, loss of life and limb. It's also possible to envision the scenario where such intrusion results in the economic collapse of the organization.

In addition to these general risks, a threat model has been developed by the National Institute of Standards (www.nist.gov) in coordination with the Process Control Security Requirements Forum and included in the document, "IT Security for Industrial Control Systems." You should note that the document indicates the list was developed using Common Criteria. Common Criteria is an international standard for developing specifications for secure information systems. You can and should visit the NIST site for more information and to follow the development of standards for process control network security. A listing of the threat model is available in the online version of this article at www.mcpmag.com.

EASY TARGETS

Process control systems are increasingly integrated with data networks, have few access controls configured and the proprietary nature of their processing doesn't block a determined attacker. In fact, the primary security for many of



A sample distributed control system (DCS) network.

these systems is obscurity, a function that only deters access. The function of these systems—even the technical operation and programming of their interfaces—is widely documented on the Internet, and former and current employees of the organizations that use them and develop them also provide a knowledge base.

In contrast, information on how to secure these systems and on the results of industry research into standards is often hard to find, requires membership in particular organizations and is protected from public quotation or reference even when publicly available.

29 THINGS YOU CAN DO

All is not lost yet, however. Many process control engineers and their IT counterparts are working on securing process control systems. They, and you, now have many places to go to learn more about process control networks and engage in a discussion of how to secure them. It turns out that securing these systems does present unique challenges, but that good security is good security no matter the system. The following list is adapted from several resources: The President's Critical Information Protection Board, the Department of Energy's "21 Steps to Improve Cyber Security of SCADA Networks," and discussions with those actively engaged in managing process control networks. The security principles pertinent to protection of data networks also have broad applicability in developing and implementing sound security policy and technical controls for process control systems and networks.

1. Don't assume the only process control networks needing security are those controlling critical infrastructure. You may not work for an electric, gas, water, communications, financial or other critical industry, but I'm willing to bet you have process control networks in your organization. They all need security.

2. Identify process control networks in your organization. You can't protect what you don't know about.

3. Document network architecture. Identify critical systems, including those that may contain sensitive information. Include process control functions such as administrative stations, gateways and intelligent devices. In addition, many process control networks have a centralized database of control information that includes configuration and data records.

4. Identify all connections to the process control networks. Connections may be via gateways to IP networks, radio, satellite, wireless, PSTN, leased line and modem. Investigate all possible connections and determine to what they provide access. Determine who has access to them and why.

5. Remove unnecessary connections. Are partner, regulatory or vendor connections necessary? Is it possible to isolate the control network? Some plant operations may reside on their own network but be arbitrarily connected to the data network. If there's no good reason for the connection, disconnect it.

6. Secure necessary connections by using available process control network gateway security, device passwords and physical security.

7. Require a review and sound security analysis to be performed on requests for new connections.

8. Implement standard, strong encryption protocols such as 128-bit AES, RSA 1024-bit and SHA-1 to ensure the integrity and confidentiality of communications, both on the process control network and in communications between it and administrative stations.

9. Require use of hardware-based keys such as smart cards, RSA tokens or USB-based devices.

10. Implement firewalls to guard access to process control networks.

11. Implement intrusion detection (IDS) systems to monitor networks and devices for unauthorized access. Provide around-the-clock monitoring.

12. Provide intrusion response "red teams" with knowledge of process control networks and how to recognize and respond to incidents. Prepare policies and procedures.

13. Remember the most basic security principal—security is only as good as its weakest link. How secure is your data network? When you protect your data network, you reinforce security for your process control networks and vice versa.

14. Remove or disable unnecessary services on process control networks

Additional Information

Organizations and resources for further information on process control systems, networks and process control security include:

- American Society for Industrial Security (now ASIS International), www.asisonline.org.
- Industrial Security Association, www.isa.org.
- The Process Control Security Requirements Forum (PCSRF), www.isd.mel.nist.gov/projects/processcontrol.
- The National Institute of Standards and Technology publications page, http://csrc.nist.gov/publications.
- U.S. Department of Energy's "21 Steps to Improve Cyber Security of SCADA Networks," www.ea.doe.gov/pdfs/21stepsbooklet.pdf.

and devices. Examples of unnecessary services may be automatic meter reading/remote billing, Web and e-mail and Internet access.

15 Require process control device and network vendors to identify secure configurations for their products and to support secure configurations of operating systems used for their devices. Examples of this are support for OS patches and software that follows OS application development standards.

16 Require vendors to support security. Secure configuration and operation shouldn't void warranty or support contracts.

17 Require vendors to disclose all backdoors, system overrides or vendor interfaces and provide the ability to block access via these.

18 Don't rely on proprietary protocols for security. These protocols can be learned as easily by an attacker as by authorized users. They may be more at risk, since they haven't been reviewed for security vulnerabilities.

19 Implement security provided by process control systems and insist on systems with security controls.

20 Perform technical audits of devices, networks and connected networks. Identify security concerns and address them. Look for active services, security patch levels, common vulnerabilities and compliance with your security policy. Re-audit systems after correcting problems. Audits should consist of inspection and penetration testing. (Be aware that common penetration testing tools may themselves disrupt service on process control systems.) Proceed with caution and test isolated or test systems. Vendors are increasing their support for the testing of patches and vulnerability testing applications in test labs at their locations. Ask for information and insist on this type of support.

21 Perform risk assessment. Develop threat models and make process control systems a part of your organization's continuing risk assessment process.

22 Include process control in your business continuity and disaster recovery plans and operations. Don't forget to back up critical configuration and data.

23 Define security roles for process control administrators, IT administrators, managers and users. Provide sufficient authority and access. Provide security awareness training that includes coverage on how to identify and avoid social engineering attacks and whom to notify for any questions

or perceived security incidents. A clear definition of response roles and responsibilities should be defined for each role.

24 Use defense in-depth. Defense in-depth is important for any security strategy. It limits the impact of a security incident, provides time for a response and may block intrusion because of the combined skills necessary to penetrate all defenses.

25 Develop and use a clear cyber security policy and program. Security for process controls must be supported by the entire organization.

26 Establish and manage proper configuration and change management, including patch management. Consistency, review and documentation are essential here. One of the largest issues in security for process control is the same as that for data systems—the management of security patches. Many of these systems run on, or are administered from, Windows systems. It may not surprise you to learn that many may still reside on Windows NT 4.0 SP3 systems. The problems may be due to a lack of patching, but they may also result from problems with proprietary device drivers that are affected by patches. This is a problem than can be resolved, but isn't going to be fixed by a simple "patch it now regardless" directive.

27 Provide physical security for process control systems, gateways, and administration stations. Provide "tamper evident" packaging and controls. An example of tamper evident packaging can be as simple as a physical lock. To open devices without a key or code, the lock must be broken. A broken or damaged lock would be evidence of tampering.

28 Obtain and highlight senior management's support and expectations for cyber security performance. Without it, any security program can fail.

29 Hold individuals accountable for their actions. The consequences of non-compliance with security policy should be clear and enforced. M

Contributing Editor Roberta Bragg, MCSE: Security, Security+ and CISSP, owns Have Computer Will Travel Inc. Her newest books are The Complete Reference: Network Security *(Osborne McGraw-Hill), and* Exam 70-298: Designing Security for a Microsoft Windows Server 2003 Network *(Microsoft Press). Contact her at roberta.bragg@mcpmag.com.*

Delegating Rights

Over the last few months, we've been discussing a variety of security-related topics. We've placed a particular emphasis on using Windows Management Instrumentation (WMI) to accomplish these tasks. However, I've always assumed that the scripts would be run by administrators such as yourselves. Proceeding under that assumption simplifies things tremendously. If only admins are running these scripts, I don't have to worry about permissions. I can assume that you have the appropriate NT permissions to perform the task, as well as adequate WMI permissions. But what if you have a script that you need users to run—one that requires a level of authority they don't have?

That was the question I received from Salvatore Cagliari, a regular reader of this column. He wrote: *"I'm facing a problem with delegation of management rights with WMI scripting. A group of users without administrative rights must be able to run VBS scripts to perform various tasks [such as] start/stop services, etc."*

He went on to say that he'd assigned the appropriate NT permissions/user rights to allow the users to start and stop the services, but the script still failed.

The good news is that you can, indeed, give a user the appropriate WMI permissions to run the script. The better news is that you maintain strict control over exactly what you allow them to do. In other words, it's not an "all or nothing" scenario. You don't have to give them the master key to your house. You can give them keys to specific rooms instead. The bad news is that you have to manage permissions in two separate places. When you think about it, though, this isn't really bad news at all. Maintaining multiple layers of security is actually a good thing.

PEELING THE ONION

The first layer of security is the one that confronts us all: NT user rights. As administrators, we have (big, booming voice, lots of reverb…) all the power in the universe! We've become accustomed to wielding this power. If we ever encounter a Permission Denied message, it causes the hair on the backs of our necks to stand up as we become filled with (righteous?) indignation. "What do you mean I don't have permission? *I am permission*!" Users, on the other hand, get these messages all the time. In order to allow them to run a WMI script to do something like the above-mentioned starting/stopping a service, we must first ensure that they have the appropriate NT permissions.

Figure 1. Use the WMI Control to allow access to specific namespaces.

The second layer is WMI itself. We must give the users specific rights to access WMI namespaces. And because WMI itself is big and complex, assigning these rights requires a certain degree of finesse. After all, we only want to enable them to perform the task we're delegating to them—nothing more. Fortunately for us, Microsoft has a tool that makes this process as easy as configuring NTFS permissions: the WMI Control.

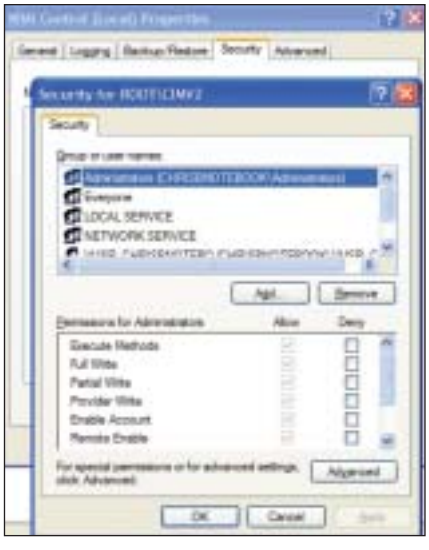


Figure 2. You can assign permission to users or groups to access WMI.

For Windows 2000/XP/2003 machines, you run

wmimgmt.msc. This opens the Microsoft Management Console (MMC) with the WMI Control loaded. The WMI Control doesn't really interact with the MMC like it should. To use it, you must either click the Properties button or right-click the WMI Control item in the treeview and select Properties. This opens the actual WMI Control application (see Figure 1). If you have NT 4.0 machines (or need to allow access to Windows 9x/ME machines), you need to run wbemcntl.exe.

For the purposes of this exercise, we're going to deal with assigning permissions to ROOT/CIMV2. This is because the CIMV2 namespace holds the Win32_Service object we need for starting and stopping services. Besides, almost every WMI script we've ever written in this column has used the CIMV2 namespace. In the WMI Control app, under the Security tab, highlight CIMV2 and press the Security button. Figure 2 shows the security dialog. This should look familiar. It's exactly like the NTFS permissions dialog, the only difference being the listed permissions. Again, because we're trying to enable users to stop and start services remotely, the permission we need to assign is Remote Access. Using the Security dialog, we simply add the user or group Remote Access to CIMV2 and all subfolders.

THEORY VS. PRACTICE

While my solution is great for Salvatore, there's no doubt many of you are scratching your heads wondering why any admin would ever give this kind of power to ordinary users. Well, let's step back and look at the big picture. Years ago, one of my servers was a test box on which we had a select group of users working. Periodically (as was often the case with NT back then), it needed a reboot in order to work properly. If I was away from my desk solving some other problem, my users were dead in the water until I came back and rebooted the server. Just think of the headaches I could have saved if users were given the ability to reboot it remotely simply by running a script.

If you think about it honestly, I'm sure you'll find lots of occasions where delegating routine tasks could make life simpler. With WMI and NT permissions working together, security need not suffer. M

Chris Brooke, MCSE, is a contributing editor for MCP Magazine *and director of enterprise technology for ComponentSource. He's been a practicing tech head for more than 15 years, specializing in development, integration services and network/Internet administration. Send questions or your favorite scripts to chrisb@componentsource.com.*

Corporate Headquarters: 9121 Oakdale Ave. Ste. 101, Chatsworth, CA 91311, www.101com.com.

Media Kits: Direct your Media Kit requests to Henry Allain, Publisher, 949-265-1556 (phone), 949-265-1528 (fax), hallain@101com.com.

Reprints: For all editorial and advertising reprints of 100 copies or more, and digital (web-based) reprints, contact RSiCopyright 651-582-3817 or cwj@rsicopyright.com

List Rentals: To rent this publication's e-mail or postal mailing list, please contact 101direct, the List Services Division of 101communications: 1-877-4-101direct (1-877-410-1347); www.101direct.com.

CONFERENCES

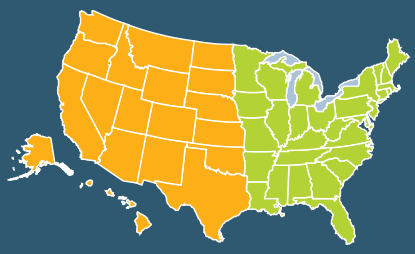
Visit www.101com.com for additional information.
SIGS/101 Conferences, and **TechMentor Conferences** contact Al Tiano, Sales Manager, 818-734-1520 ext. 190, atiano@101com.com.
The Data Warehousing Institute contact Diane Smith, Exhibit Sales, 206-246-5059, ext. 108, dsmith@dw-institute.com; Denelle Hanlon, Publication and Sponsorship Sales, 206-246-5059, ext. 102, dhanlon@dw-institute.com.
FCW Events and Conferences contact Lucy Cooley, Events Director, 703-876-5081, lcooley@101com.com.
Syllabus Conference and Exhibition, contact Anne Morris, Exhibit Space or Sponsorship, 818-734-1520 ext. 219, amorris@101com.com.

Microsoft Certified Professional Magazine (ISSN: 1081-3497, USPS: 0015-657) is published monthly by 101communications LLC, 9121 Oakdale Avenue, Ste. 101, Chatsworth, CA 91311. Periodicals postage paid at Chatsworth, CA 91311, and at additional mailing offices. Regular annual subscription rates for U.S.$39.95 (U.S. funds). Postage for Canada/Mexico $15 (U.S. funds); and International $25 (U.S. funds).
Subscription inquiries, back issue requests, and address changes: Mail to: *Microsoft Certified Professional Magazine*, P.O. Box 2063, Skokie, IL 60076-7963 or call (866) 293-3194 for U.S. and Canada, (402) 293-9134 for International, fax (847) 647-9295.
POSTMASTER: Send address changes to *Microsoft Certified Professional Magazine,* P.O. Box 2063, Skokie, IL 60076-7963. GST (Canada) #R891450934; Canada Publications Mail Agreement No: 40039410. Return Undeliverable Canadian Addresses to Circulation Dept. or DPGM 4960-2 Walker Road, Windsor, ON N9A 6J3.

ADVERTISING SALES

HENRY ALLAIN, PUBLISHER
949-265-1556 PHONE
949-265-1528 FAX
HALLAIN@101COM.COM

MATT N. MOROLLO
ASSOCIATE PUBLISHER
508-875-6644 EXT. 18 PHONE
508-875-6633 FAX
MMOROLLO@101COM.COM



West

HI, AZ, UT, TX, NV, CO, NM, OK, CA, NE, KS, ND, SD, WY, MT, ID, OR, WA, AK, BC, ALBERTA, SASKATCHEWAN, MANITOBA, PACIFIC RIM, AUSTRALIA, NEW ZEALAND, INDIA, PAKISTAN

DAN LA BIANCA
WESTERN REGIONAL SALES MANAGER
818-674-3416 PHONE • 818-734-1528 FAX
DLABIANCA@101COM.COM

East

MN, IA, MO, AK, LA, WI, IL, MS, MI, IN, OH, KY, TN, AL, GA, ME, NH, VT, MA, RI, CT, NY, PA, NJ, DE, MD, WV, VA, NC, SC, FL, QUEBEC, ONTARIO, EUROPE

JD HOLZGREFE
EASTERN REGIONAL SALES MANAGER
804-550-0169 PHONE • 253-595-1976 FAX
JDHOLZGREFE@101COM.COM

IT Certification & Training – USA, Europe

ABBY ZIFF
ADVERTISING SALES MANAGER,
IT CERTIFICATION & TRAINING
703-876-5132 PHONE • 703-876-5142 FAX
AZIFF@101COM.COM

Online Sales – ENTmag.com and TCPmag.com

TANYA EGENOLF
ADVERTISING SALES MANAGER
760-722-5494 PHONE • 760-722-5495 FAX
TEGENOLF@101COM.COM

Production

NIESHA ALEXANDER
PRODUCTION COORDINATOR
818-734-1520 EXT. 210 PHONE
818-734-1528 FAX
NALEXANDER@101COM.COM

AD INDEX

EDITORIAL INDEX

MCP RESOURCES

GENERAL RESOURCES	INTERNET & TELEPHONE
Microsoft Training and Services	www.microsoft.com/traincert (800) 636-7544
E-mail alias for MCP questions	MCPHelp@microsoft.com
Microsoft TechNet	www.microsoft.com/TechNet (800) 344-2121
Microsoft Press	http://mspress.microsoft.com (800) MS-PRESS
Microsoft CTEC referrals	www.microsoft.com/traincert/training/find (800) 765-7768
Prometric exam registration	www.2test.com (800) 755-3926 (952) 820-5707
VUE exam registration	www.vue.com/ms (800) 837-8734

The publisher assumes no liability for errors or omissions.

Renewal Notice

Auntie was reflecting on her past career as business development manager for a company that made niche Web tools (our biggest seller: Bowser, Internet Explorer retooled for pooches) while paying a few domestic bills the other day. At least, that's my excuse for being startled when dear Fabio murmured in my ear. "Jumping the gun on that one a bit, aren't you?" he inquired gently.

Looking down, I noted that I was writing a check for a magazine subscription renewal that wasn't due until 2008. This is one of those magazines that sends out renewal reminders every month—whether you need to be reminded or not—and, well, they snag the occasional daydreaming writer of opinion columns.

This little playlet got me thinking about Microsoft certifications (as do many things when I've got a column to write). Microsoft says that over 1.5 million people have achieved Microsoft certification. That should be no surprise to those of you who read the other pages of this very magazine. The question in Em's mind is how many of you have come back for those subscription renewals in the form of another round of the same credential.

As you probably know, Microsoft started versioning the MCSE credential with Windows NT 4.0, and now you can be an MCSE on NT 4.0, Windows 2000 or Windows 2003. The MCSD certification is also versioned: You can get it with or without .NET. And in a year or two, I expect MCDBAs will face the equivalent choice, as there will probably be a SQL Server 2005 MCDBA alongside the existing SQL Server 7.0 and 2000 versions. If administrators, developers and DBAs were lemmings, this would be a fabulous thing for Microsoft; they'd rake in the bucks as we dutifully took every new exam.

However, the evidence says that lemminghood is in relatively short supply out here in the real world. Microsoft doesn't release a full statistical analysis of its certifications, but you can draw some conclusions from the number of folks with each certification, which they do publish. Only about 60 percent as many people got the Windows 2000 MCSE as the Windows NT 4.0, and so far, the Windows Server 2003 certification has comparatively minuscule numbers (though it's been out less than a year).

Over in application land, the story appears to be much the same: Around a thousand developers have picked up the original MCSD every month, but in its first year, the MCSD .NET only averaged about 600 developers each month. And some of those are certainly new customers rather than repeats. What's everyone else waiting for?

If you've been around the certification universe for awhile, this isn't particularly surprising. Repeat sales in certification are far from guaranteed for any vendor. Some folks will inevitably be disappointed when the promised fame and fortune don't materialize after their first certification. These people are poor prospects for an upgrade. Others will pragmatically decide not to upgrade because, in most cases, it doesn't matter. When was the last time a prospective employer bothered to check your assertion that you were certified, let alone the version you claimed?

But such pragmatism has its drawbacks. Upgrading to the latest version of any certification has the same benefits we're always preaching for getting certified in the first place—it validates your skills and forces you to study your subject broadly. So if it was good to certify, it's good to renew, right? In that case, though, why aren't more of you doing it? Perhaps it's true that the effort follows the money—that if you don't see financial gains, you won't bother.

Or maybe the newer exams are just too tough. Over the years, it's gotten harder to get a Microsoft certification—so maybe more of you are still in the pipeline on your way to the next big title. Or perhaps it's just a sign of increasing age and forgetfulness. On your glorious path to becoming your organization's go-to systems engineer, you just plain forgot about recertifying. In which case, isn't it time to register for some exams now…just in case? M

What's your personal certification renewal policy? Are you still sneaking around with an MCSE on Windows NT 3.51? Drop a line to Auntie@mcpmag.com.

Quest Software and Aelita Software have come together.

The Active Directory and Exchange experts have united. To make your life easier. To deliver comprehensive solutions that simplify, automate and secure your Microsoft infrastructure. By working with the experts and using proven solutions, you will improve the productivity, system availability and security of your Windows enterprise.

> ***"The people and products from Quest and Aelita are one. One team of experts. One vendor that will provide our customers the best solutions for managing their Microsoft infrastructure."***
>
> Ratmir Timashev, General Manager
> Microsoft Infrastructure Management
> Quest Software

Now you can manage the complete lifecycle of your Microsoft infrastructure. You can administer, migrate, troubleshoot, recover, and audit. All with solutions from one source. All supported by an industry-leading team of Windows experts.

Together, Quest and Aelita bring you:

- Comprehensive set of Microsoft infrastructure management solutions
- Leading team of Active Directory and Exchange experts
- Complete lifecycle management capabilities
- One partner for your Windows enterprise

When you learn from the experts, you win.
Visit our **Library of White Papers**
at www.quest.com/microsoft/win

For more information visit www.quest.com/microsoft or call Quest at 800-263-0036. You'll discover solutions that combine the features you want with the performance you need to simplify, automate, and secure your Windows enterprise.

aelita SOFTWARE *is now a part of* QUEST SOFTWARE®

Microsoft GOLD CERTIFIED Partner | Active Directory | Exchange | Windows | Migration |