Office Communications Server p. 24 ■ Market Watch: Web Conferencing p. 29

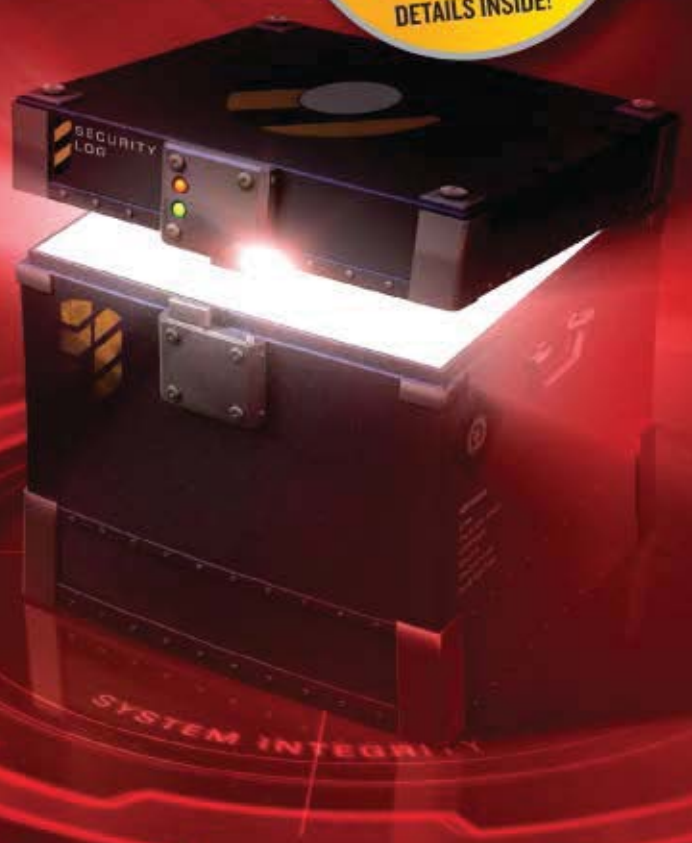
MANAGEMENT • SECURITY • NETWORKING • MESSAGING • HOW-TO

Windows® IT Pro

We're in IT with You

It's Time to Deploy UC! DETAILS INSIDE!

Unlock the SECRETS of the SECURITY LOG p. 36



PowerShell Scripting:
Easy GPO Management p. 46

Ready for IPv6? p. 51

Exchange 2007 Information Store:
Stability and Performance p. 57

Mark Minasi's Windows Power Tools p. 77

REQUIRED READING
Plan Vista Deployment with BDD p. 63

OFFICE & SHAREPOINT PRO
MOSS 2007 Business Data Catalog p. 69

Penton
A PENTON PUBLICATION
OCTOBER 2007
WWW.WINDOWSITPRO.COM
U.S. $5.95 CANADA $7.95

_INFRASTRUCTURE LOG

_DAY 79: This is out of control! Our IT environment is rigid and inflexible. Our business needs are changing, but our environment isn't built to change with them. We can't adapt. Oh, no...I was afraid of this. We're so rigid we're stuck in time.

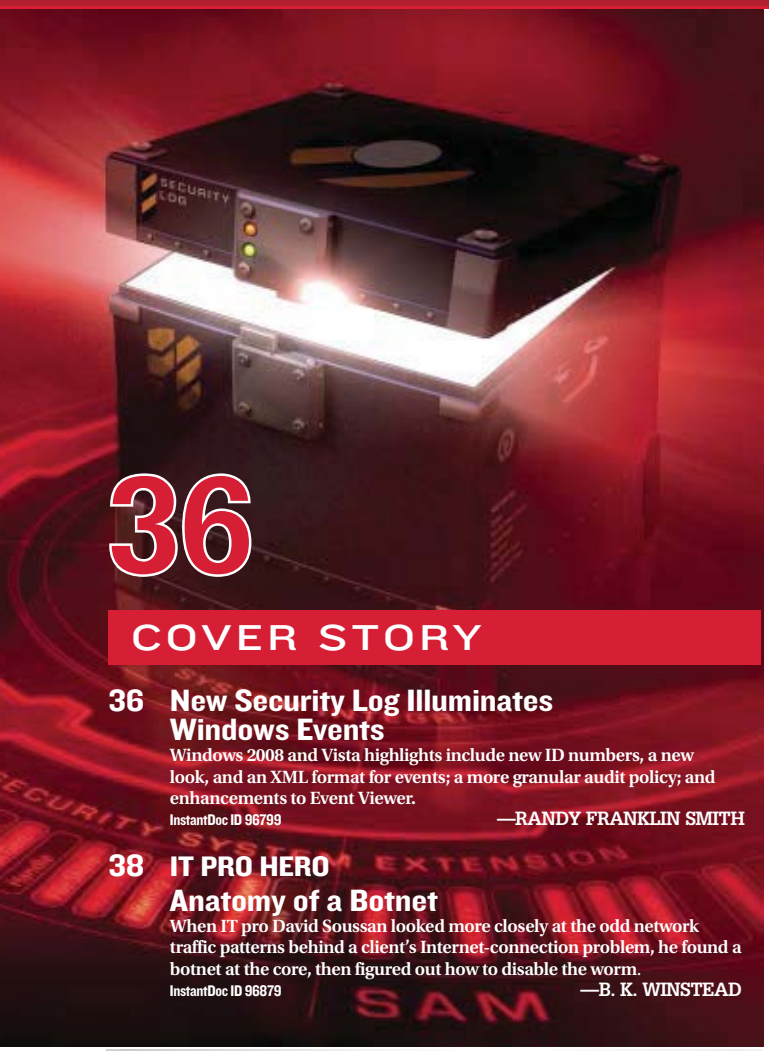
_*Infrastructurus prehistoricus*. I've read about this.

_DAY 80: I'm taking back control with IBM SOA solutions. Now we can align business goals with our IT. We have the hardware, software and services we need to respond to change. Strategy, planning and implementation are in tune with our specific business needs. Now we can deploy and update business processes faster and more efficiently.

_Goodbye, rigid past. Hello, flexible future.

Take the SOA business value assessment at:
IBM.COM/**TAKEBACKCONTROL**/SOA

Windows IT Pro
OCTOBER 2007 VOLUME 13 NO. 10

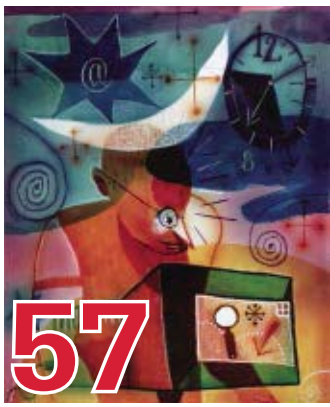


36

COVER STORY

FEATURES

FEATURES



REQUIRED READING: WINDOWS VISTA

OFFICE & SHAREPOINT PRO

WEB EXCLUSIVES

COMPARATIVE REVIEW

VPN Firewalls for SMBs
Three network security appliances, one Editor's Choice—these VPN firewall appliances from **NETGEAR**, **SonicWALL**, and **ZyXEL Communications** include stateful packet inspection that can detect DoS attacks.
InstantDoc ID 95955 —JOHN GREEN

Collaborate Using Office OneNote 2007
Use OneNote 2007 to drive team participation and enhance communication by creating a shared digital notebook to capture ideas and share information.
InstantDoc ID 96577 —WILL KELLY

COLUMNS

Karen Forster
IT Pro Perspective
Exchange 2007 SP1 and PerformancePoint
With Software Plus Services, Microsoft ups the ante in its competition with Google and SaaS. The company still has to protect revenue from traditional software, but it also has a strength competitors can't match. InstantDoc ID 96977

Paul Thurrott
Need to Know
Paul takes a look at the long-overdue SP3 for Windows XP, then comments on the new features and improvements (and more than a thousand bug fixes) found in the latest Windows 2008 CTP release. Finally, Paul gives us his take on Microsoft's chances to dethrone Adobe Flash as the premier rich Internet content delivery system with the new Microsoft Silverlight.

COVER PHOTO BY

TRICKS & TRAPS

PRODUCTS

WHAT'S HOT

IN EVERY ISSUE

» Learning Path Article not a perfect fit? Find more resources to match your knowledge and skills.
Network with authors, peers, product vendors, and Microsoft.

HIT MALWARE. HARD.

NEW V2! Now with VIPRE™ Technology

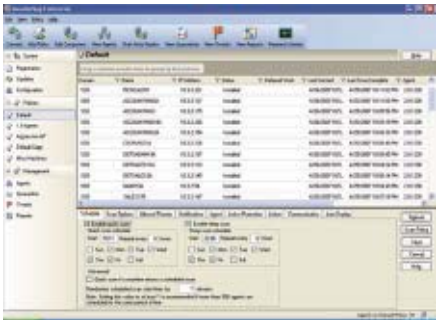
Windows IT Pro READERS CHOICE 2006 Winner

2006 Network Computing WELL-CONNECTED AWARDS WINNER

Product Excellence Awards 2007 Info Security Products Guide CUSTOMER TRUST

Is your network protected against blended malware threats? Cyber criminals are using combinations of spambots, worms, trojans, rootkits and social engineering to infect your users' machines. Spyware has morphed into malware. You need protection against these new security threats.

Surveys show one of the biggest security issues admins see this year is blended malware. Protecting your network from the loss of confidential data, employee productivity, and network bandwidth is a major issue.



CounterSpy Enterprise: The most powerful antimalware available: Company-wide malware protection requires a real, centralized enterprise product. CounterSpy Enterprise is just that: a scalable, policy-based tool that delivers a new, revolutionary hybrid antimalware technology that provides robust protection against blended threats.

Hybrid antimalware engine with VIPRE technology: CounterSpy Enterprise is powered by a hybrid engine that merges classic spyware detection and remediation with Sunbelt's new Virus Intrusion Protection Remediation Engine. VIPRE has traditional antivirus and cutting-edge antimalware techniques. The upshot? Faster scanning and dramatically less system resources.

Kernel level Active Protection: CounterSpy Enterprise's Active Protection™ offers signature, behavioral and heuristic-based real-time blocking of threats. It works seamlessly with existing desktop antivirus solutions. And it has the best threat database in the industry. Period.

Download your evaluation copy at:
www.sunbeltsoftware.com/csewin

Sunbelt Software

COUNTER SPY ENTERPRISE

Find out how many machines in your organization are infected NOW!

Sunbelt Software Tel: 1-888-688-8457 or 1-727-562-0101 Fax: 1-727-562-5199 www.sunbeltsoftware.com sales@sunbeltsoftware.com

windowsitpro.com

"Taming the Beast: Gain Control of Software Usage and Reduce Audit Risks"

Organizations face serious challenges related to vendors' licensing models, such as cost overruns, missed deadlines and business opportunities, and lost user productivity. Learn how to address these challenges and prepare for audits.

http://www.windowsitpro.com/go/seminars/macrovision/softwarelicensing/?partnerref=citcoct

IT 911: Experts and Resources When You Need Them

When you need information about an event that could affect your network, the IT 911 blog is required reading. *Windows IT Pro* authors and editors give you the information you need and provide expert insight and real-world experience to help you make the right decisions.

http://www.windowsitpro.com/go/IT911

"Consolidation for Optimized Windows File and Print Serving"

Explore how you can save money on your storage solution by using existing hardware, learn how to implement scalable Windows-based clustered NAS on a shared data framework, and discover techniques for leveraging existing network infrastructure and management processes with a shared data architecture.

http://www.sqlmag.com/go/seminars/polyserve/consolidation/?partnerref=citcoct

"Messaging Management"

A secure messaging infrastructure is crucial to your business. This eBook introduces three messaging management services—security, availability, and control services—and explains how to implement them in a Microsoft-centric messaging environment.

http://www.windowsitpro.com/go/ebook/symantec/messagingmanagement/?code=citcoct

YOUR SAVVY ASSISTANT

by Christan Humphries

If you think the only content we have is what you see in our print magazine, you haven't been paying attention. Our print magazine is just a sliver of the information we offer. For example, if you're not seeing the Exchange content you want in this issue, check out these great resources online:

Need to Know Guides

I bet you didn't realize how much you need these quick references.
"Top 7 Tips for Deploying Exchange Server 2007"
"Top 7 Exchange Disaster Recovery Tips"
http://www.windowsitpro.com/needtoknow

Essential Guides

What else can I say? "Essential guides" is pretty self-explanatory.
"Exchange 2007 High Availability and Disaster Recovery: What You Get and What You Need"
"Continuous Data Protection for Exchange"
"Real-Time High Availability for Exchange"
http://www.windowsitpro.com/essential

Alan Sugano's Web-Exclusive Content

More like "Alan Su-*guru*." Alan writes tons of helpful articles that seem to fly under the radar.
"Exchange Event 1023 IMAP4SVC Error," InstantDoc ID 95862
"Getting Your iPhone to Sync with Exchange 2003," InstantDoc ID 96730
"Can I Upgrade to Microsoft Exchange Server 2007 from Exchange Server 5.5?" InstantDoc ID 95611

Podcast: Exchange 2007 and High Availability

Paul Robichaux talks about Exchange Server 2007's new clustering and replication features and what they mean to your HA design as you prepare to migrate. He also highlights HA situations that might be better addressed by other technologies.
http://www.windowsitpro.com/go/ExchangeHA

Exchange & Outlook Pro VIP

This one's a no-brainer. *Exchange & Outlook Pro VIP* is the essential information source for Microsoft Exchange and Outlook pros. Members get access to technical articles, Q&As, forums, and scripts. You should join; all the cool kids are.
http://www.exchangeprovip.com

The Crucial Flaw in Server Performance

Today's server technology is designed to withstand critical workloads. But there is still one major flaw, and a secret edge for solving it.

The Importance of Server Reliability

It's important enough that a single user is able to rely on a computer, and that the user's data is always there and quickly retrievable. But when that computer is a server, and when the number of users escalates from one or a few up to thousands, the word "important" as it relates to reliability and uptime becomes a severe understatement. In today's corporate world, servers are the brains and backbones of the enterprise, for executives, employees and, most importantly, customers and prospects. Even a few minutes of server slow-down or downtime impacts the bottom line of the company.

A large part of the reason that server reliability has become so vital is the evolution of the Web. No longer the static display that it once was, the Web is now a place where billions in commerce is conducted, where buyers shop for commodities, pricing and availability, and where customers log in to place and track orders. CRM applications, once only used for internal employees on the phone, now interface with Web applications so that customers and even employees can interact with the company online. Databases such as SQL must be instantly responsive, as these interface with the Web as well.

Server Technology Evolves to Keep Up—Almost

Server technology has some time since passed the point of being single-box/single-disk solution, having migrated into solutions such as SAN (Storage Area Networks), providing scalability, redundancy, reliability, and performance. Technology such as virtualization takes server computing one step further, making more efficient use of resources for greater power to deliver data and services. Chip technology such as quad-core is being marketed to keep pace with the constantly rising need for processing power.

But despite all these advances, the cornerstone to server response remains the hard drives, as they remain the slowest components — the "weakest links." Unfortunately emerging technologies such as virtualization don't change that fact, and actually exacerbate it. While being the weakest links, disks are also the storehouse for all server applications and data. Keeping those drives defragmented for optimum performance has long ago become a "given"[1] — but it's the defragmentation technology that can make the crucial difference between keeping drives at maximum performance and simply "functioning." With today's frantic pace of 24/7 server disk access, fragmentation is continuous and

constant, and scheduled defragmentation does not keep pace[2]. To keep fragmentation from corrupting workflow, you truly need **Diskeeper® 2007** with its proprietary InvisiTasking™ technology defragmenting your disks, constantly and invisibly, with no hit on system resources.

"Diskeeper has transparently prevented disk fragmentation from building up and measurably slowing down our production servers. The ability to prevent fragmentation from building up without impacting CPU load on the servers has been a key feature of the product."

William Cox, IT Director, Georgia Department of Easy Care and Learning, Atlanta, GA

InvisiTasking: The Secret Edge to Server Performance

As thousands of IT personnel throughout the world have discovered, **Diskeeper 2007 Server**, with its proprietary breakthrough InvisiTasking technology, defragments and enhances file systems in real-time, with no scheduling needed. Testing has shown that scheduled defragmentation leaves fragmented files behind after running, or in best cases only provides a very short respite from performance loss. Only **Diskeeper 2007** consistently eliminates fragmentation to continuously provide maximum performance and reliability — automatically[2].

"I am very pleased with [the improved] performance I am seeing on the Windows® 2003 servers we have **Diskeeper 2007** installed and running on. SQL creates and deletes many temporary tables. Setting up the defrags to be automatic, the SQL performance increased substantially. Queries that originally took 30 seconds or so are completing in 5 – 10 seconds. The only change was having **Diskeeper 2007** installed and operating."

Richard B. West, Systems Management Architect, IT Solutions and Infrastructure Engineering, Melbourne, FL

Diskeeper EnterpriseServer version also contains advanced technologies such as Terabyte Volume Engine™ 2.0.

"Previously we were unable to defragment the terabyte arrays and fragmentation was resulting in processing delays of incoming data files. This resulted in our SQL server falling behind during times of high usage. Now, thanks to Diskeeper, we have breathing room to handle future growth."

Julie McGowan, Santa Cruz County, CA

The backbone of enterprise computing environments is the server. And disk subsystems are, undoubtedly, vital to the overall performance of a server. And as tens of thousands have discovered, the most essential component for maintaining maximum performance and reliability of those drives is **Diskeeper 2007 Server** editions. Take advantage of the free 45-day trial and see for yourself.

Special Offer

Diskeeper 2007
Maximizing Performance and Reliability —*Automatically!*™

Automated with NEW InvisiTasking™

Try Diskeeper 2007 FREE for 45 days!

Download: www.diskeeper.com/wit8

(Note: Special 45-day trialware is only available at the above link)

Volume licensing and Government / Education discounts are available from your favorite reseller or call 800-829-6468 code 4414

[1] File Fragmentation White Paper www.diskeeper.com/paper3

[2] White Paper: Is Real-Time Defrag Needed? www.diskeeper.com/paper4

Diskeeper corporation

Exchange 2007 SP1 and PerformancePoint

A new competitive model for Microsoft?

When Microsoft recognizes a challenge, the wheels of change start spinning faster than a politician's PR team cleaning up after a nasty indiscretion. A challenge the company is now tackling at that furious pace is the perception that Microsoft can't compete with Google and Software as a Service (SaaS).

To address this challenge, Microsoft is integrating its individual products with Web components in a model it calls Software Plus Services to create end-to-end solutions such as unified communications (UC) and business intelligence (BI). This competitive strategy is coupled with company-wide adoption of System Center and Windows PowerShell for an integrated management model. Recent announcements, especially of Microsoft Exchange Server 2007 SP1 and Microsoft Office PerformancePoint Server 2007, are interesting in light of this integration.

Exchange 2007 SP1

When Microsoft explains its Software Plus Services vision, the company invariably holds up the model of Exchange Server's integration with the Outlook client and Outlook Web Access. But Exchange's role in Microsoft's future strategy goes beyond email into the realm of the next "killer app," UC. The August announcement of a Community Technology Preview (CTP) of Exchange 2007 SP1 pounded home the UC message, stating, "SP1 will drive added value for our customers, further establishing Exchange Server as the foundation of a unified communications platform," which includes email, voicemail, IM, and voice and video communications.

According to Ray Mohrman (group product manager, UC), SP1 adds support for Windows Server 2008 and Windows Vista. SP1 lets you manage Exchange from a Vista machine by using PowerShell, Microsoft Management Console, and the Exchange Server Best Practices Analyzer. Additional SP1 features include new Microsoft ActiveSync policies for synchronization, authentication, and encryption. SP1's Standby Continuous Replication feature uses Exchange's log file shipping to continuously replicate mailbox data to a standby server, which can quickly be activated if the primary server is offline. In the area of security, SP1 integrates with Forefront Security Server SP1 and provides IPv6 support with Server 2008.

But the focus of the announcement seemed to be on integration with Microsoft Office Communications Server 2007 (OCS—the heart of the company's UC product line). SP1 enables one-click retrieval of voicemail messages from the OCS client, Microsoft Office Communicator 2007, and allows Communicator and Communicator-enabled phones to alert users to new voice messages.

The importance of SP1, according to Microsoft, is in "addressing the overall communications and collaboration needs of companies." With the complete UC solution, Microsoft has a competitive position that Google and SaaS competitors can't approach: a comprehensive set of products that can be assembled as end-to-end solutions, starting with the OS and extending through the communications infrastructure to systems management, data and storage, and end-user productivity.

PerformancePoint

Microsoft quotes IDC's research finding that the overall BI market grew by more than 11 percent in 2006, while Microsoft's BI revenue grew 28 percent, the highest growth rate among the top 10 industry players. For Microsoft, BI isn't just an opportunity to release new products such as PerformancePoint. Rather, BI represents an opportunity to sell a solution that consists of several individual products: Windows Server and Microsoft SQL Server on the back end, with Microsoft Office PerformancePoint Server 2007 and Office applications such as SharePoint and Excel on the front end. Don't be surprised to hear soon about how Microsoft's BI solution will have Software Plus Services components and System Center–based management.

Together at Last

The biggest obstacle Microsoft faces to competing with Google and SaaS is its business model. Microsoft can add online services to its software products but, unlike Google, still has to protect revenue from traditional software.

However, Microsoft has a strength that none of its competitors (except perhaps IBM) can touch: a broad range of products that can be assembled to form end-to-end solutions. Most important, Microsoft has an experienced customer base that has already invested in learning Microsoft skills. That skill base makes it easier and cheaper for customers to stick with Microsoft than to invest in learning non-Microsoft products.

By unifying the Microsoft stack with a common management model and providing end-to-end solutions, Microsoft is betting that it can leverage its mature and emerging products and build on existing customer knowledge to outflank competitors. What do you think? Is it more cost effective to adopt Microsoft's solutions than to try out competitive offerings? I'd love to hear whether you agree.

InstantDoc ID 96977

Karen Forster (karen@windowsitpro.com) is editorial and strategy director for *Windows IT Pro* and *SQL Server Magazine* and former director of Windows Server User Assistance at Microsoft.

Did You Know?

The Microsoft Unified Communications roadshow is coming to a city near you, and your registration includes a one-year subscription to *Windows IT Pro*. Go to http://www.windowsitpro.com/go/ucweb for details.

_INFRASTRUCTURE LOG

_DAY 89: Our power and cooling costs are out of control! These boxes throw off so much heat. The energy costs are staggering. We're spending the bulk of our IT budget just keeping the data center cool. I told Gil we need to go green in a big way.

_DAY 91: Gil made the data center green. Kelly green, to be exact. There's got to be a better way.

LVR's Intricacies

Thank you for Guido Grillenmeier's article "Leverage LVR to Simplify AD Object Recovery" (August 2007, InstantDoc ID 96310). Guido deepened my understanding of Active Directory (AD) and how it replicates. I might have to read the article a couple of times to fully understand everything, though.

As I was reviewing my AD groups to see if they contain Linked Value Replication (LVR) links, I ran into an interesting find with the default group Domain Users, which most of our users have as their primary group. When I run the command

```
repadmin /showobjmeta DC1
  CN="Domain Users",
  CN=Builtin,OU=XYZ,OU=COM
```

it returns information only about the users who do not have Domain Users set as their primary group. If I go into an individual user account and change the primary user group, the individual shows up when I rerun the command.

- Why don't user accounts show up when their group is set to primary?
- Since I can't see the LEGACY, ABSENT, or PRESENT status for the users, can I assume that all the LVR links are PRESENT?

—Justin Marthaler

I'm glad you liked the article. The topic is fairly complex.

The Domain Users group is a special group just like Domain Computers and a few others in AD. As you noted, those groups' membership is typically not explicit by virtue of the user (or computer) being listed in the group's memberOf attribute. Instead, the member's PrimaryGroupID attribute is populated with the Relative Identifier (RID) of the respective AD group (513 for Domain Users). This attribute is indexed so that the OS can list all members quickly.

The Active Directory Users and Computers GUI fools you by displaying the users as normal members of the Domain Users group. When you check the memberOf tab for a user, it also displays the Domain Users group. The GUI basically checks both the backlinks and the PrimaryGroupID, just like the logon process does to add the group to a user's token. This process allows an AD domain to contain as many users (or computers) as you want and not be limited by the number of members or forward links that could fit into a group's memberOf attribute.

When you change a user's primary group, the same logic is applied to the other group: The user's link is removed and instead the group's RID is written to the user's PrimaryGroupID attribute. But because you didn't remove the Domain Users group when you edited the user's PrimaryGroup, an explicit link is added to the Domain Users group.

So basically, a group that's populated with the PrimaryGroup feature doesn't use LVR. However, it works similarly in that it allows very large groups and only the membership change is replicated.

—Guido Grillenmeier

I just read "Leverage to Simplify AD Object Recovery" and liked it a lot. I hope more people will buy into taking LVR and the related issues more seriously once they or some of their staff have read the article.

—Scotty McLeod

Enhanced Defrag

Dan Gillard's article "Automate the Windows 2003 Defragmenter Without Paying Extra" (Reader to Reader, May 2007, InstantDoc ID 95487) made me wonder: Why not just use defrag.exe, which is a command-line tool that ships with Windows Server 2003 and Windows XP and can be easily scheduled with Task Scheduler? Does it offer less functionality than dfrgntfs.exe?

—Chris Munger

The batch file uses defrag.exe to launch dfrgntfs.exe. I don't use defrag.exe directly with the Task Scheduler because this process runs on a file server, and usually no one is logged on to the server. For a scheduled task to work when no one is logged on, you need a username and password that has admin rights to run the task. For all I know there might be a way to hack into the task scheduler to get passwords, and I'd rather not have that.

Instead of having a process run by a user who has admin rights on the server, I use the AT command to run the command like a service without a logon account. This approach also runs the process in the background and prevents windows from popping up.

The log file this batch file creates also is a good way to check for problems after the defrag process has run. Defrag.exe itself doesn't create a log unless you output the process to a text file.

The batch file I created is just another means to defrag the system, with extra features.

—Dan Gillard

Mysterious Behavior of the Windows Indexing Service

Thank you Bret Bennett for sharing in detail what you learned about the Windows Indexing Service ("An Unlikely Culprit Can Cause Computers to Hang," August 2007, InstantDoc ID 96343), and thank you *Windows IT Pro* for printing it. That article is a good example of why I subscribe to the magazine.

—Chris Hair

InstantDoc ID 96931

EDITOR'S NOTE

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

Help make your data center green with IBM Cool Blue™ technologies and energy management services.

Go green with virtualization: *Advanced server and storage virtualization from IBM can help you decrease your number of boxes and lower your energy usage.*

Go green with energy management: *IBM Systems Director can give you active energy management to help you track and cap your power consumption.[1] It can help you see and regulate how much power the systems in your data center are really using.*

Go green with more efficient systems: *IBM POWER6™ processors with Advanced Power Virtualization mean your systems can use less energy doing the same amount of work.[2] For instance, consolidating 30 Sun V890s into one rack of POWER6-based IBM System p™ 570s can save you over $100K a year in energy costs alone.[3]*

Go green with IBM: *IBM Services can help design your data center, holistically, for better energy usage. With outstanding technology and people who understand what that technology can do for your business, IBM can help make your data center green.*

Learn how to make your data center more efficient.
IBM.COM/**TAKEBACKCONTROL**/GREEN

1. Currently available on IBM System x and IBM BladeCenter servers. Expected to be available on IBM System i and System p servers 11/07. Energy management capabilities of IBM Systems Director are not available on IBM System z. 2. Advanced Power Virtualization is optional and available at an additional charge. 3. For complete details, go to ibm.com/takebackcontrol/claim.

Manage Any Data Center. Anytime. Anywhere.

SEE US AT ANY OF THESE SHOWS!

Infrastructure Mgt. World
Scottsdale, AZ - Booth TBD
Sept. 10 - 12

VM World
San Francisco, CA - Booth 1113
Sept. 11 - 13

AFCOM Data Center World
Dallas, TX - Booth 436
Sept. 17 - 18

High Perf. on Wall Street
New York, NY - Booth 216
Sept. 17

IDC Enterprise Infra. Forum
New York, NY - Booth TBD
Sept. 20

Interface Salt Lake City
Salt Lake City, UT - Booth 309
Oct. 4

GEOINT
San Antonio, TX - Booth 374
Oct. 22 - 24

Interop New York Fall
New York, NY - Booth 543
Oct. 24 - 25

AFCEA Asia-PAC TechNet
Honolulu, HI - Booth 516
Nov. 4 - 9

Super Computing
Reno, NV - Booth 164
Nov. 12 - 15

LISA
Dallas, TX - Booth 200
Nov. 14 - 15

DaCEY Awards
Atlanta, GA
Nov. 15

Gartner Data Center Conf.
Las Vegas, NV - Booth TBD
Nov. 27 - 30

Interface Seattle
Seattle, WA - Booth 206
Nov. 28

Avocent builds hardware and software to access, manage and control any IT asset in your data center, online or offline, keeping it, and your business, "always on".

Visit us on our Remote Control Tour. For locations near you, go to **www.avocent.com/remotecontrol.**

Avocent®
The Power of Being There®

What You Need to Know About ...

Windows XP SP3

Since Microsoft shipped two service packs for XP (one of them a major OS upgrade) within the product's first few years on the market, it's somewhat surprising that, three years after SP2, we've yet to see an SP3 release. Microsoft is working on XP SP3 but is being quite cagey about when it will be available. Here's what you need to know about XP SP3.

Why the Delay?

Despite Microsoft's enormous size (more than 77,000 employees and roughly $50 billion in annual revenues), in some cases the company's organizational structure actually constrains which products are actively developed. Although a large team of developers, product managers, and program managers is involved in the ramp-up to any major OS release, Microsoft then pushes the product to its support organization for follow-up development in the form of hotfixes, service packs, and so on. Other teams work on out-of-band updates that are typically released via the Web, and eventually a new or existing team is constituted to work on the next major release and the entire process begins anew.

In the case of XP, however, Microsoft was forced to temporarily halt development on Windows Vista in order to complete SP2 because it was, in fact, a major OS upgrade and was developed outside of the company's support structure—a first for any service pack. After SP2 completion, Microsoft dedicated every available employee to Vista, which by that time was years behind schedule. In early 2007 Microsoft finally reassigned employees to the development of XP SP3.

What SP3 Includes

Whereas XP SP2 was an enormous release with dramatically improved security features, Microsoft says that SP3 will be a more typical service pack with no major new features. So SP3 will include a roll-up of all the hotfixes, security fixes, and other updates that have been released since SP2, as well as the contents of SP1 and SP2, as is typically the case.

Recommendation

Microsoft plans to release XP SP3 in the first half of 2008. Given the relative security, stability, and reliability of SP2 and the subsequent release of Vista, XP SP3 might seem like a pointless update, but nothing could be further from the truth. Many businesses will roll out new XP-based PCs in the coming years, and as anyone who's had to update an XP SP2 system can tell you, the 100-plus updates that Microsoft has shipped since SP2 can be a nightmare to deploy. If you're already running XP and have been regularly updating those systems, the release of SP3 will be a minor event. But if you've planned XP deployments for the future, look very carefully at this release and consider it the baseline for your next generation of PCs. Or, you could decide to go the Vista route, which will be supported with updates much longer than XP will. Incidentally, SP3 will also be available via Windows Update.

InstantDoc ID 96859

Paul Thurrott (thurrott@windowsitpro.com) is the news editor for *Windows IT Pro*. He writes a weekly editorial for *Windows IT Pro UPDATE* (http://www.windowsitpro.com/email) and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (http://www.wininformant.com).

What You Need to Know About...

Changes in Windows 2008 Since Beta 3

In April 2007, Microsoft shipped Windows Server 2008 Beta 3, a major milestone on the road to its next server OS. This release includes a slew of new features, which I examined two months ago in Need to Know (See "What You Need to Know About Windows Server 2008 Beta 3," August 2007, InstantDoc ID 96068). Since then, however, Microsoft has refreshed this product with a new Community Technology Preview (CTP) build that includes even more new features and functionality while fixing almost a thousand bugs. Here's what you need to know about what's changed in Windows 2008 since Beta 3.

The Big News: A Web Server Role

The biggest and most exciting change is that Windows 2008 Server Core will now support a Web Server role, a feature that was missing from previous beta releases. Originally, Microsoft didn't expect to be able to ship a Web Server role for Server Core, which lacks support for the Microsoft.NET Framework, necessary foundational technology for ASP.NET, and other IIS features. To get around these limitations, Server Core's Web Server role just doesn't support ASP.NET, so if you need it or other .NET-based technologies in IIS, you'll have to install the

Did You Know?

Find out more about Windows Server 2008 on Paul Thurrott's SuperSite for Windows: http://www.winsupersite.com/showcase/win2008_ntk.asp.

full version of Windows 2008. Note, however, that classic ASP does work on Server Core, according to Microsoft.

The reasons for making a version of the Web Server role without ASP.NET available to Server Core users are excellent, however. The role gives Microsoft shops a low-cost, small-footprint alternative to Linux Web servers, for example, and still provides all the core Web server functionality one could need. You can also put non-Microsoft Web server technologies, including Apache and PHP, on top of such an installation. And since Server Core is the least resource-intensive and most secure version of Windows 2008, you get those benefits as well. Of course, you'll also need to master the command line, but that's another story.

Smaller Changes and Updates

Another post–Beta 3 change is an update to Microsoft Windows Media Services (WMS) that basically provides compatibility with the latest prerelease versions of Windows 2008. As its name suggests, WMS is a media server that lets you stream Windows Media–based content across a network.

Beyond that, most of the changes you'll see in post–Beta 3 builds of Windows 2008 are performance improvements, fit and finish changes, bug fixes, and other small improvements. Post–Beta 3 versions of Windows 2008 are available to beta testers, MSDN subscribers, and TechNet subscribers, so if you qualify, be sure to grab the latest version of this impressive system.

Recommendation

If you have access to a more recent prerelease version of Windows 2008 than Beta 3, you should immediately begin evaluating that version of the product instead of Beta 3. Although Beta 3 was ostensibly "feature complete," in fact Microsoft has made some changes since then and has fixed hundreds of bugs. Windows 2008 is a huge and important upgrade to Microsoft's venerable server line and one that you'll want to be up on sooner rather than later.

InstantDoc ID 96860

What You Need to Know About...

Microsoft Silverlight

Credit Microsoft for being an excellent creator of platforms. Its Windows, Microsoft .NET, and Microsoft Office products are industry standards, and the company has made important inroads with Microsoft IIS, Windows Mobile, and many other products. On the Web, Microsoft Internet Explorer (IE) is the de facto standard, despite a slew of formalized Web standards, and even Microsoft's oft-criticized ActiveX technologies are widely deployed worldwide. With regard to Web rendering technologies, Microsoft hasn't been much of a presence, but the company hopes to change its standing with a new technology called Microsoft Silverlight, which is essentially a platform for developing rich applications that run in the browser. Here's what you need to know about Silverlight.

What It Is; What It Isn't

Although often compared to Adobe Flash technology, which provides basic animation, UI, and data display features, Silverlight is in fact dramatically more powerful and extensible. Consider just the ability to deliver video over the Web: With Flash, developers are stuck with the low-resolution, low-quality video users have come to associate with such video sites as YouTube. But Silverlight provides access to HD, full-fidelity video at a reliable 700Kbps of bandwidth. Microsoft will even host up to 4GB of video for users at no cost.

However, Silverlight isn't just about video. In conjunction with the release of this technology, Microsoft is also opening up new APIs for its various Windows Live services, including Live Search, Virtual Earth, and Windows Messenger. As a result, developers who target Silverlight will be able to access Microsoft's large and growing collection of back-end services from their Web applications.

From a programming perspective, Silverlight applications utilize .NET managed code and can be expressed in Extensible Application Markup Language (XAML), the XML-based markup language that Microsoft created for Windows Vista. XAML applications can be written using a simple text editor, or more preferably by using a graphical tool that creates XAML code, and are thus open for inspection by Web search engines and other online tools. This is another point that contrasts with Flash, which is essentially a closed "black box" environment. And because Silverlight is being targeted at Apple's Safari and Mozilla's Firefox browsers as well as IE, it should work on just about any computing platform, including Macintosh and Linux. (Most Silverlight developers will of course create their applications in Windows.)

Silverlight provides access to HD, full-fidelity video at a reliable 700Kbps of bandwidth. Microsoft will even host up to 4GB of video for users at no cost.

Ultimately, what really sets Silverlight apart is the quality of the UIs you can create and the continued use of XAML, which is particularly easy to parse and automate with various designer tools. Whether it will translate into real-world success is hard to know. Certainly, Microsoft's track record with cross-platform browser add-ins has been poor at best.

Recommendation

If you're looking at rolling out Web applications that will access back-end data and you're working in a primarily Microsoft-based shop, do take a look at Silverlight. The first version should be shipping by the time you read this, but Microsoft is already offering an early public beta of the next version and will likely continue to update the technology.

In the current online world, in which many sites are transitioning into so-called Web 2.0 applications, Silverlight is only one of several competing technologies. But it offers numerous advantages for those who are wedded to Windows on the server and development sides. It's definitely worth investigating. For more information, visit the Silverlight Web site at http://silverlight.net/GetStarted.

InstantDoc ID 96861

Time-Saving Tips for Typing URLs in IE

Microsoft Internet Explorer (IE) 7.0 is a great browser. It has many new features, most of which are security-related. However, there is one new feature that can simplify your browsing experience.

Most people know that instead of typing a full URL in IE's address bar (e.g., http://www.mywebsite.com), you can simply type the domain name (e.g., mywebsite) and press Ctrl+Enter. IE then automatically adds the *http://www* prefix and *.com* suffix. Most all browsers, including earlier versions of IE, offer this feature.

Apostolos Fotakelis

If you often visit .com sites and sites that have a national suffix, IE 7.0 has a feature you'll want to check out.

In IE 7.0 and IE 6.0, you can customize the suffix, which is *.com* by default. First, you need to create a QuickComplete registry subkey under the HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Toolbar key. Then, in the QuickComplete subkey, you need to create a registry entry with the following properties:

Name: QuickComplete
Type: REG_SZ
Value: http://www.%s.net

As you might have noticed, both the subkey and entry have the same name (i.e., QuickComplete), which is a bit unusual. Although this example changes the suffix to *.net,* you can change the suffix to whatever you need.

Besides *.com* sites, many international users also visit sites that have their national suffix. For example, many users in Greece also visit sites that have the *.gr* suffix. IE 7.0 has a little-known feature than can help such users. Start IE 7.0 and follow these steps:

1. Select Internet Options on the Tools menu.
2. Click Languages.
3. In the Suffix box, type the suffix you want (e.g., gr).
4. Click OK twice.

Now, when you want to enter a site that has a *.com* suffix, you just enter the domain name and press Ctrl+Enter. When you want to enter a site that has the national suffix (e.g., .gr), you just enter the domain name and press Ctrl+Shift+Enter.

—Apostolos Fotakelis, Systems Administrator, Aristotle University of Thessaloniki, and freelance IT consultant

InstantDoc ID 96852

A Fast Yet Secure Way to Open MMCs Using Alternative Credentials

Like Serge Bédard in the Reader to Reader article "Access Remote Files with iexplore.exe" (June 2007, InstantDoc ID 95445), I also use a standard account for logging onto my workstation and a high-privilege account for performing network-related tasks in various Microsoft Management Consoles (MMCs). Constantly using the Run As command to open the MMCs with the high-privilege account proved to be tedious and time-consuming. To reduce the amount of time spent entering alternative credentials, I wrote a series of batch files for the following consoles:

- Active Directory Users & Computers (adusers.msc), which is a customized console for the MMC Active Directory Users and Computers snap-in that has all our domains loading in one pane
- MMC ADSI Edit (adsiedit.msc)
- MMC Computer Management (compmgmt.msc)
- DHCP (dhcp.msc), which is a customized console for the MMC DHCP snap-in that has all our DHCP servers loading in one pane.
- DNS (dns.msc), which is a customized console for the MMC DNS snap-in that has all our DNS servers loading in one pane.
- Group Policy Object Editor (gpedit.msc)

The batch files are pretty simple. They typically look like the batch file in Listing 1, which opens the Active Directory Users & Computers console. When the batch file executes, all you need to do is provide the password for your privileged account. The console then opens and loads the appropriate snap-in.

The batch file to open the Computer Management console is slightly different. As Listing 2 shows,

Listing 1: Batch File That Opens the Active Directory Users & Computers Console

```
@Echo Off
Cd\
c:
Runas /user:privileged_id@domain.com "mmc.exe
  \\networkpath\adusers.msc"
Exit
```

Listing 2: Batch File That Opens the Computer Management Console

```
@Echo Off
Cd\
c:
Set /P server=Please enter the server to connect to:
Echo.
Runas /user:privileged_id@domain.com
  "mmc.exe \\networkpath\compmgmt.msc /computer:%server%"
Exit
```

EDITOR'S NOTE

Share your Windows discoveries, comments, solutions to problems, and experiences with products and reach out to other *Windows IT Pro* readers (including Microsoft). Email your contributions to r2r@windowsitpro.com. Please include your phone number. We edit submissions for style, grammar, and length. If we print your submission, you'll get $100. Submissions and listings are available online at http://www.windowsitpro.com. Enter the InstantDoc ID number in the InstantDoc ID text box.

this batch file first prompts you for a server name, then prompts you for the privileged account password. If both are correct, the Computer Management console opens with that computer name already loaded.

To make it easy to execute the batch files, I placed them on a network share, along with the console files they're linked to. I then created shortcuts to the batch files on my Quick Launch bar. So, to run an MMC, all I need to do is click the appropriate shortcut and enter the password (or server name and password).

The batch files turned out to be so convenient that I wrote a set of them for each member of our IT team. These batch files not only save our team a ton of time but also help us comply with the company's administrative security policies.

—Joel Hluszko, Senior Network Administrator, Kingsway Financial Services

InstantDoc ID 96854

Export AD Data into Access So Users Can Run Their Own AD Reports

If your organization is anything like mine, you get daily requests from managers for information about the users, computers, and groups in Active Directory (AD). These requests can be simple (e.g., "Can I get a list of all users who are in the New York office?") or detailed (e.g., "Can I get a list of all users with mailboxes on SERVER1 who haven't logged in since April?"). And managers often come back asking for slightly different information or for the information to be presented in a slightly different way. This leaves you—the busy administrator, who has servers to maintain and projects to complete—spending a lot of time tweaking and rerunning scripts.

One skill necessary to be a successful administrator is finding ways to provide people with the means to help themselves, while ensuring that they don't have the ability to break something. Given this goal, I developed a solution that gives managers an easy way to obtain custom AD reports without them having to directly access AD or learn how to write scripts. I export relevant AD data into a Microsoft Access database (although you can just as easily export the information into a SQL database). With this tool, managers can easily run a custom report and tweak it until it returns the data they need in a format they like.

To build this reporting tool, you first need to create a database in Access. If you're unfamiliar with Access, Microsoft offers a series of free Access 2003 courses at http://office.microsoft.com/en-us/training/CR061829401033.aspx. For our purposes, I created a sample database that has a single table named ADUsers with four fields: DisplayName, UserID, EmailAddress, and UserDisabled. Each field is a default text field with the exception of UserDisabled, which is a yes/no field. One note of caution: When you're creating your database, make sure the field lengths are large enough to store the information you're gathering. Some AD attribute values are quite long (e.g., dn) and won't fit into Access's default field length. You can download the sample database, ADUsers.mdb, from the *Windows IT Pro* Web site. (Go to http://www.windowsitpro.com, enter 96855 in the InstantDoc ID text box, then click the *Download the Code Here* hotlink.)

Now it's time to write the script.

Listing 3: PopulateDB.vbs

```
On Error Resume Next
Option Explicit
Dim objCommand, objConnection, strQuery, strDBPath, objRecordset
Dim objAccessConnection, objAccessRecordset, objItem
Const ADS_UF_ACCOUNTDISABLE = 2
Const adLockOptimistic     = 3

' Connect to AD.
Set objCommand = CreateObject("ADODB.Command")
Set objConnection = CreateObject("ADODB.Connection")
objConnection.Provider = "ADsDSOObject"
objConnection.Open "Active Directory Provider"
objCommand.ActiveConnection = objConnection
A strQuery = "<LDAP://dc=mycompany,dc=com>;(objectCategory=person);" _
   & "adsPath;subtree"
objCommand.CommandText = strQuery
Set objRecordset = objCommand.Execute

' Open the Access database.
Set objAccessConnection = CreateObject("ADODB.Connection")
Set objAccessRecordset = CreateObject("ADODB.Recordset")
B strDBPath = "c:\ADUsers\ADUsers.mdb"
objAccessConnection.open ("DRIVER=Microsoft Access Driver (*.mdb);DBQ=" & strDBPath)
Set objAccessRecordset.ActiveConnection = objAccessConnection
objAccessRecordset.LockType = adLockOptimistic

' Delete all the rows from the database so it can be repopulated.
objAccessRecordset.source = "DELETE * FROM ADUsers"
objAccessRecordset.Open
objAccessRecordset.source = "Select * FROM ADUsers"
objAccessRecordset.Open

' Loop through all the user accounts and insert their details into the database.
C Do Until objRecordset.EOF
   Set objItem = GetObject(objRecordset.Fields ("ADsPath"))
   objAccessRecordset.AddNew
   objAccessRecordset.Fields("DisplayName") = objItem.displayName
   objAccessRecordset.Fields("UserID") = objItem.sAMAccountName
   objAccessRecordset.Fields("EmailAddress") = objItem.mail
     If objitem.userAccountControl And ADS_UF_ACCOUNTDISABLE Then
       objAccessRecordset.Fields("UserDisabled") = True
     Else
       objAccessRecordset.Fields("UserDisabled") = False
     End If
     objAccessRecordset.Update
   objRecordSet.MoveNext
Loop
```

Top 10 Tips for EFFECTIVE Compliance Management

When you think of compliance management, you probably first think about electronic records such as email messages and IM conversations. However, those records are only the tip of the iceberg: there may be many other potential compliance pitfalls that you need to investigate, and possibly remedy, in your environment. Here are the Top 10 Tips to help you meet your compliance needs and stay on top of them.

Tip 1: Know your industry.

There are several tiers of regulatory requirements that may apply to you. These will vary depending on where your company operates, what industries it works in, and what kind of business it does. In addition to international and national compliance regulations, many industries have specific compliance requirements that you must meet. For example, if you work for a bank, mortgage company, brokerage, or other financial-services company, there are industry-specific objectives you must meet. Even for small companies in largely unregulated sectors, there's an emerging consensus that the best protection is the ability to show that you know and follow commonly accepted industry best practices for security and compliance management. Make sure you understand these best practices and that you can show how they've been applied in your environment.

Tip 2: Define measurable objectives.

In your environment, it may not be possible to patch every system instantly when a security fix is released, and it may not even be possible for you to regularly audit the configuration of every machine. Whatever your compliance needs, you must define measureable objectives that you can use to see how well your compliance plan is operating. You'll need a way to measure the success rate of your patching operations, as well as tools to report on configuration changes that were, or were not, authorized.

Tip 3: Trust but verify.

When Microsoft and other vendors release security patches, they test against a wide range of systems and applications. However, that doesn't mean that the patches have been tested against your systems and applications. Before blasting a software update out to your entire organization, it's wise to make sure that you've tested it on a representative sample of your critical systems. In fact, you should make this a core part of your compliance strategy so that you don't cause problems while trying to solve them.

continued on back

Tip 4: Spotlight critical resources.

Not all systems are created equal—and you shouldn't treat them as though they were. Of course, it's important to define and enforce a baseline standard of protection across all your computers, because compromise of even a single system can lead to more widespread problems. However, your most critical assets—the ones your business can't run without—should be given special attention, monitoring, and treatment. Identifying these systems will help you focus on protecting your most important assets (always, of course, following vendor guidelines for which categories of systems need particular patches in what order).

Tip 5: Quantify your risks.

To make effective risk decisions, you need to have hard data on what risks you really face and what their potential impacts are. The only way to get this is to perform an in-depth risk assessment. There are many tools to help you get started, but the easiest way is to simply list your risks—system breaches, loss of confidential data, and so on—and rank them by the amount of expected damage. Once you have that list you can quantify the expected loss, and the probability that the risk will occur, more precisely.

Tip 6: Scan regularly.

Your network is always changing, whether or not you know it. Even in a highly managed environment, computers come and go on the network. It's essential that you make regular scans of your network to assess which machines are there, what applications and services they offer, configuration compliance, what software they have installed, and what patches they do—or don't – have.

Tip 7: Practice change management.

One of the reasons commercial air transportation is so safe is that mechanics, pilots, and maintenance staff all keep insanely detailed written records about every change they make to an aircraft. You can do the same thing, and reap many of the same benefits. Your best bet is to automate the process as much as possible by using reporting and monitoring tools to keep track of what changes are made. For this to be effective, administrators need to get in the habit of tracking the changes they make so they can be reviewed later. (Bonus points if you also confine changes to specified periods so that you lower the risk of breaking critical services during working hours.)

Tip 8: Audit key items.

You probably already have auditing procedures in place for security-related events, but how good are they? How good are your admins at following them properly? At a minimum, you should be auditing account changes, grants of administrative privileges on the OS and your applications, and major configuration changes. If possible, you should expand the scope of your auditing to include changes related to your compliance policies and procedures.

Tip 9: Document what you do.

Whatever you do, don't consider it "done" until you've documented it. Documentation is a key part of change management, and it's also an important part of demonstrating that you're handling both parts of compliance: having a documented process, then sticking to it.

Tip 10: Watch the news.

Compliance requirements can change quickly, spurred by events like major data losses or widespread malware attacks. To ensure that your compliance management strategy keeps you protected, you'll need to stay on top of security news, but not just from your software vendor. Try to develop contacts within your industry to help give you a wider early-warning net, too.

Listing 3 shows a sample script named PopulateDB.vbs, which you can also download from the *Windows IT Pro* Web site. After the script declares the variables and constants, it connects to and queries AD. As callout A in Listing 3 shows, an LDAP query is used. You need to modify this query to reflect your actual domain configuration. LDAP queries include three or four arguments, which are delimited with colons:

- You use the mandatory first argument (in this example, <LDAP://dc=mycompany,dc=com>) to specify where in AD you want to start the search. You must use a full path and enclose it in angle brackets (< >).
- You use the mandatory second argument, which must be enclosed in parentheses, to specify the objects to search for. For example, the *(objectCategory=person)* argument in Listing 3's query tells the script to search for all user objects derived from a class whose defaultObjectCategory attribute is person.
- You use the mandatory third argument to specify the attribute to return. In this example, it's the ADsPath attribute, which is used later in the script to bind to each AD user object returned by the query. You can customize the query to return any number of attributes. When you have more than one attribute, you put the attributes in a comma-delimited list.
- You use the optional fourth argument to specify how far down from the query's starting point you want to search. The options are Subtree (checks every container in the tree), OneLevel (checks objects directly under the root and objects directly under containers in the root), and Base (only checks objects directly in the container).

After executing the query and storing its results in the objRecordset variable, PopulateDB.vbs connects to Access and opens the ADUsers database. In the code at callout B, you need to customize the path to ADUsers. The script then deletes all the records in the database. The database is cleared each time so you don't have to have to search for existing records and determine whether those records have been updated.

In the code at callout C, the script loops through all the AD user objects in the objRecordset variable. After binding to each object using its ADsPath, the script retrieves the values of the displayName, sAMAccountName, mail, and userAccountControl attributes. For each attribute value, the script adds a new record to the database.

To run PopulateDB.vbs, open a command-shell window and run the command

```
cscript c:\ADUsers\PopulateDB.vbs
```

The database can't be open when you launch the script. If it's open, the script will fail. I wrote and tested this script on Windows XP SP2 with Access 2003.

Once all the information is in the database, it's simple to sort and query the data because Access is designed for that purpose. If your managers aren't familiar with Access, you'll need to teach them the basics. Although training them will initially consume some of your time, the return on this investment is worth it because you'll no longer have to spend time every day writing and tweaking scripts for managers.

Listing 4 shows some sample queries for the ADUsers database. The first example generates a list of all disabled user accounts. The second example illustrates how to filter that list so only disabled user accounts that have an email address are selected.

Listing 4: Sample Queries for the ADUsers Database

```
-- Example 1: Query that generates a list of all disabled user accounts
SELECT ADUsers.DisplayName, ADUsers.UserID, ADUsers.UserDisabled
FROM ADUsers
WHERE (((ADUsers.UserDisabled)=True));

-- Example 2: Query that generates a list of disabled user accounts
-- that have email addresses
SELECT ADUsers.DisplayName, ADUsers.UserID, ADUsers.EMailAddress,
  ADUsers.UserDisabled
FROM ADUsers
WHERE (((ADUsers.EMailAddress) Is Not Null) AND ((ADUsers.UserDisabled)=True));

-- Example 3: Query that generates a list of home directories
-- that are no longer in use
SELECT HomeDir.HomeDir
FROM HomeDir LEFT JOIN ADUsers ON HomeDir.HomeDir = ADUsers.UserID
WHERE (((ADUsers.UserID) Is Null));
```

As ADUsers and PopulateDB.vbs demonstrate, you can build a robust reporting tool by importing relevant AD information into a database that people can use to run their own reports. Because you'll no longer have to continually write and rewrite reporting scripts, you'll have more time left for important tasks, such as keeping your environment up to date and secure. In fact, you can even use this tool for some of those tasks. For example, if your users' home directory names match their user IDs, you can use the tool to determine which home directories are no longer in use. You just need to create an additional table named HomeDir, populate a field called HomeDir with a text list of all home directories on your servers, and run the third sample query in Listing 4. The query results will show you the records from HomeDir that don't have user IDs in ADUsers, which indicates those home directories aren't being used.

Managers will like the AD reporting tool because they can easily run customized reports. You'll like it because you'll have more time to keep your environment up to date and secure.

—Chris Scoggins

InstantDoc ID 96855

Jeff James (jjames@windowsitpro.com) is senior editor, products, for *Windows IT Pro* and *SQL Server Magazine*. He specializes in virtualization and terminal services and has over 15 years of experience as a writer and digital-content producer.

SharePoint Management

Control SharePoint Access and Permissions

Managing access control policies for SharePoint is the focus of **Securent**'s Entitlement Management Solution 3.0. This new version of the software is the first entitlement management product to support Windows SharePoint Services 3.0 and Microsoft Office SharePoint Server 2007. The new release enables enterprises to establish, manage, and monitor access control policies to SharePoint resources such as Web content, search queries, individual documents, and document libraries. For more information, call 650-625-9400 or go to http://www.securent.com.

Remote Administration

Manage Clients and Servers Remotely

Matrix42 has announced the release of Empirum Remote Control 3.0, an update to its remote systems management software. In addition to allowing administrators to remotely manage servers and client computers, the new version employs an improved compression process to enhance performance during remote system access. The software also introduces support for Web cameras, real-time chat, and VoIP for remote administration sessions. Users can integrate Remote Control 3.0 into their existing Matrix42 Empirum product architecture or use the application as a standalone product. For more information, contact Matrix42 at 404-923-8380 or visit the company's Web site at http://www.matrix42.com.

Product Spotlight

Exchange Backup

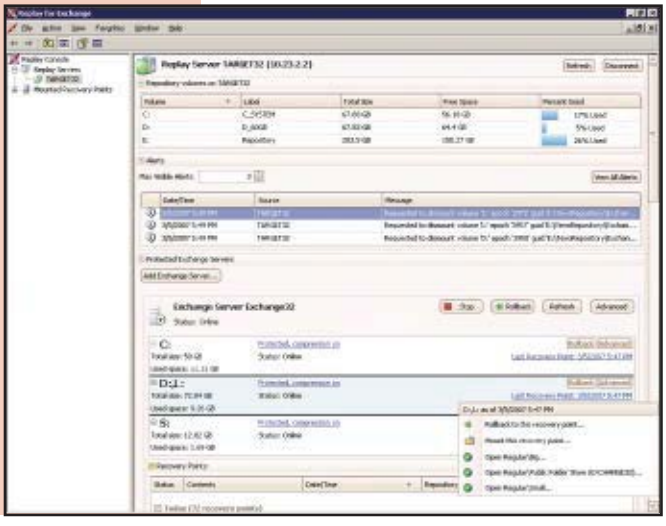
Protect and Recover Exchange Server Data

In an effort to simplify data backup and recovery on Microsoft Exchange Server systems, **Appassure** has unveiled Replay for Exchange. This new application promises to give Exchange admins some extra resources to keep their Exchange server ecosystems protected against catastrophic failures and to simplify the search and recovery of Exchange data.

Appassure CEO Najaf Husain claims that Replay for Exchange is the "only real-time Exchange backup and recovery solution that lets you roll back Exchange from a single message to the entire server—to any point in time—in just minutes." Backup and recovery speed is a key feature of the product, allowing admins to quickly recover Exchange servers corrupted by bad data, malware, viruses, and other glitches. That capability also drills down to the individual mailbox level, allowing admins to search and restore individual email messages directly to existing Exchange mailboxes or PST files, all with a few mouse clicks.

Replay for Exchange works independently of your network, storage, and server hardware and is compatible with virtualization technologies from Microsoft and VMware. It also fully supports both x86 (32-bit) and x64 (64-bit) platforms.

Replay for Exchange starts at $1,995 for mailbox servers; licenses for domain controllers and additional Exchange 2007 role servers are $795 apiece. For more information, contact Appassure at 703-547-8686 or go to http://www.appassure.com.



Document Management

Create and Manage Secure Documents

Workshare has released Workshare Professional 5, the latest update to its document control product. The new version provides support for document life cycle management in Microsoft Office 2007 and Windows Vista and improved protection from information leaks. The company claims that Workshare

An Amazing Breakthrough in E-Discovery and Recovery.

...FOR EXCHANGE

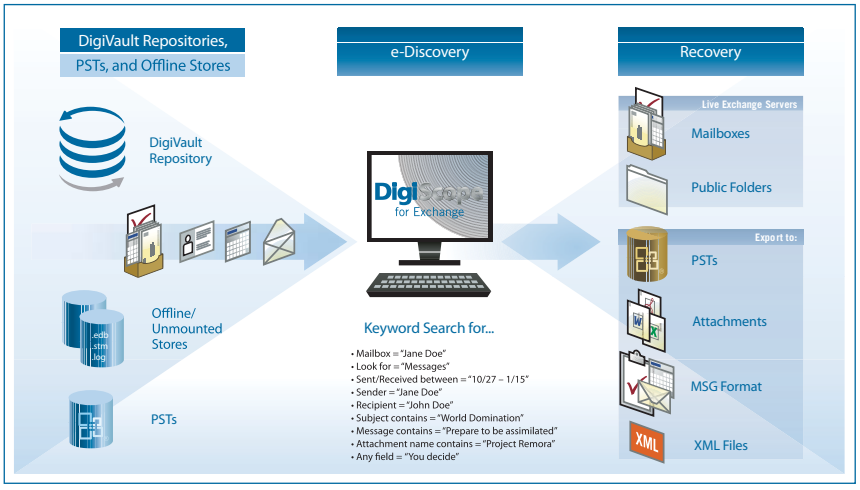
Makes Complex, Time-Consuming and Expensive E-discovery and Recovery a Thing of the Past.

DISCOVER – DigiScope's robust and flexible search capabilities enable you to rapidly query one or more Exchange databases, PST files, or DigiVault™ data sets to locate a specific mailbox, folder, e-mail item, or entire conversation thread in record time.

RECOVER – Easily restore individual mailboxes, folders, messages, contacts, schedules, and other e-mail items directly to your production Exchange server, or extract the required data into a PST, MSG, XML, or native attachment file format for transport, review, regulatory compliance, or Legal hold.

RELAX – With DigiScope, you can quickly find and recover invaluable lost, deleted, or historical data without implementing never-ending mailbox brick-level backups, costly Exchange recovery infrastructures, or ineffective Recovery Storage Groups.

How it Works



FREE DOWNLOADS

- Demo version of DigiScope
- White Paper –"The Federal Rules of Civil Procedure, E-mail Discovery and You." by Osterman Research

Go to: www.Lucid8.com/Discover
Call: 425 456-8493
E-Mail: Sales@Lucid8.com

Microsoft® GOLD CERTIFIED Partner

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

Created by Lucid

Solutions Inspiring Confidence

EDITOR'S NOTE: Send new product announcements to products@windowsitpro.com.

Professional is the first product to generate and manage security-enhanced, leak-proof PDF documents. Other new features include the ability to track document changes (with changes now stored separately from the source file) and a One-to-Many DeltaView feature that allows easy comparison of multiple documents and their changes and versions. A one-year license for Workshare Professional is $175 per user; perpetual licenses are $349 per user plus annual maintenance. Other pricing options and upgrade discounts are also available. For more information, contact Workshare at 415-975-3855 or visit the vendor's Web site at http://www.workshare.com.

Backup and Recovery

Manage Mixed-Media Backup and Recovery

Symantec recently announced an update to Veritas NetBackup, which lets network admins use one tool to manage a variety of backup storage media, including tape, disks, and virtual tape libraries. New features include enhanced support for disk-based backup, native data deduplication, operability with intelligent backup appliances, and granular data recovery for virtual machines and enterprise applications. A capacity-based pricing model is also available. NetBackup 6.5 is a key part of Symantec's Storage United platform, which includes Veritas Enterprise Vault and Veritas CommandCentral Storage. For more information, contact Symantec at 408-517-8000 or go to http://www.symantec.com.

Virtualization Management

Manage Virtualized Resources

Virtualized resources are presenting new management, security, and compliance challenges, which **Configuresoft** hopes to address with the release of its Configuration Intelligence for Virtualization platform. Configuration Intelligence for Virtualization centralizes and automates security, configuration, auditing, and monitoring of virtual as well as physical assets. Dashboards show security and compliance status at a glance across the entire physical and virtual environment. For more information, contact Configuresoft at 719-447-4600 or visit http://www.configuresoft.com.

Security

Tackle Security and Event Management

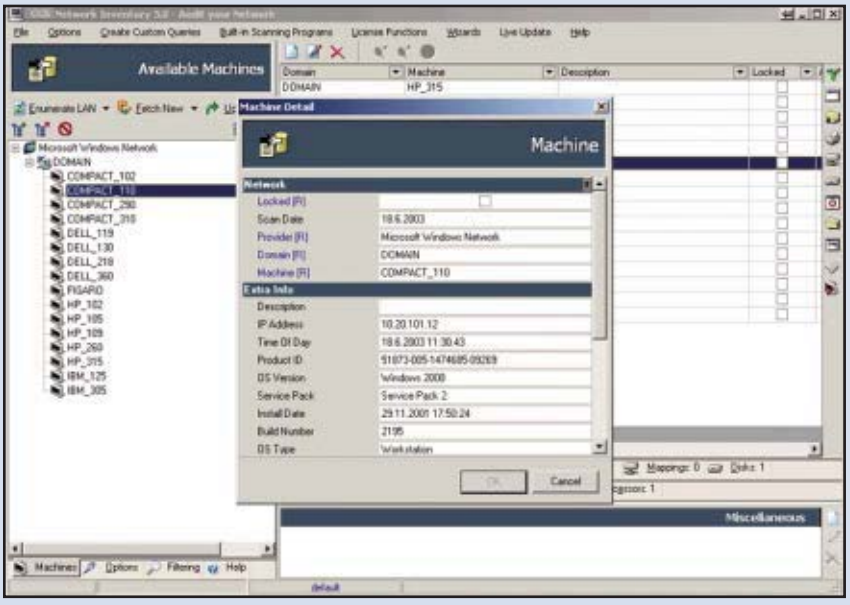
With system security, auditing, and regulation-compliance demands pressuring IT administrators, vendors such as **NetIQ** are responding with products that consolidate, monitor, and archive data generated by complex security infrastructures. With the release of NetIQ Security Manager (SM) 6.0 with Change Guardian for Windows, NetIQ tackles user monitoring, change auditing, and threat detection. SM uses Microsoft's file system filter drivers and includes TRACE, a proprietary log management technology. For more information, contact NetIQ at 919-767-0200 or visit http://www.netiq.com.

InstantDoc ID 96800

Network Administration

Streamline Network Inventory Tasks

To ease one of the more thankless tasks of IT administrators, **Crow Canyon Systems** has introduced CCS Network Inventory. At definable intervals, an auto-discovery option finds and records new and changed assets in the network. The product integrates with Crow Canyon's Outlook HelpDesk, which helps optimize the process of identifying and resolving user requests for assistance. For more information, contact Crow Canyon Systems at 707-746-5272 or visit http://www.crowcanyon.com.



Insights from the industry

PostPath Offers Linux-Based Microsoft Exchange Alternative

Migrating to Microsoft Exchange Server 2007 is a huge undertaking. Because Exchange 2007 is a 64-bit application, new hardware is necessary in most cases—and costly. In addition, organizations are worried about the complexities of migrating (e.g., having to redo their Active Directory—AD—topologies), as well as the time involved in migration. According to a survey conducted by Osterman Research, 66 percent of organizations considering a migration to Exchange 2007 are concerned about the cost. These factors may lead some companies to look for more affordable alternatives to Exchange 2007, such as **PostPath** Server.

According to PostPath, its product is the first third-party product to be natively compatible with Microsoft Office Outlook and Microsoft Exchange Server. This Linux-based email and collaboration server runs on 32-bit architecture and aims to reduce your messaging costs. PostPath looks like Exchange on your network because it uses the same low-level (i.e., Messaging API) protocols that Exchange and Outlook use to communicate, and it provides high-availability disaster recovery and presents fewer synchronization problems than Exchange, the company says. PostPath also provides low-cost storage. For example, you can put a group of users on a $1,500 server and attach a $3,000 4TB storage unit, rather than buy several new $10,000 servers.

PostPath doesn't require you to change your existing infrastructure, nor do you need a dedicated administrator. You can install the product at a remote location, with no administrator, and have the server back up asynchronously over a low-bandwidth connection. And according to Scott Young, PostPath's VP of marketing, users will never know that you've switched their email system.

Scott also says that PostPath doesn't "lock you into a particular environment [or] define what other applications you can use." For example, the product supports open-source applications, standards-based SMTP, and even Asynchronous JavaScript and XML–based Web clients.

PostPath is geared toward large and mid-sized Linux-friendly Windows shops. Scott says the product offers these organizations "the best of both worlds ... the ability to keep their existing desktops the same but then have a lower-cost, higher-performance back end."

Although PostPath isn't significantly cheaper than Exchange, it can preempt or at least delay your move to Exchange 2007. PostPath's research shows that 31 percent of organizations are still running Exchange Server 5.5, so the company has developed a guide to help admins migrate directly from Exchange 5.5 to PostPath. A free 12-user license is available, so you can try the server (or even use it in a very small company). For more information, go to http://www.postpath.com.

—Lavon Peters

InstantDoc ID 96670

Solidcore Partners with Neoware, Inks Deal with Opsware

Change management control software vendor **Solidcore Systems** has been very busy in the 3rd quarter, managing to ink a sales and marketing pact with Opsware, move its headquarters to Cupertino, California, and win some large customers for its change control software in just a few months. Now Solidcore has announced that it's joined forces with Neoware to integrate Solidcore's S3 Control - Embedded software with Neoware's thin-client computing solutions.

In a statement issued in support of the partnership, Neoware Executive Vice President of Sales Jim Kirby stated that working with Solidcore will "help ensure our systems are not compromised by any unauthorized software changes" and improve customers' ability to manage and centralize information across their IT infrastructures. Kirby also explains that Solidcore's change control features allow the Neoware products that use them to eliminate emergency patching and reduce Help desk support costs for customers.

Solidcore's agreement with Opsware—which was recently acquired by HP for a whopping $1.6 billion—is more noteworthy and shows that the company continues to gain traction in the change control software market. In a recent briefing, Solidcore's VP of Marketing Bob Vieraitis stressed that the agreement with Opsware demonstrated the validity of his company's approach, noting that Solidcore's S3 – Control product was the only third-party program that Opsware currently resells.

Vieraitis mentioned that a key benefit of the integration of S3 Control with the Opsware Systems 6 data center automation suite was the ability to monitor and respond to infrastructure change in real time. "We bring the ability for real-time tracking and analysis of change management to Opsware," says Vieraitis. "Keeping track of change in real time is important ... we can track all changes in real time and reconcile those changes in real time. [Our solution] can issue reports on demand, all in an effort to keep our customers in continuous compliance."

This latest partnership indicates that Solidcore's embedded change control product continues to gain customers. The company's S3 Control products are used by developers of a wide variety of hardware in vertical markets, ranging from storage appliances and automated teller machines to point-of-sale terminals and medical devices. For more information about Solidcore, go to http://www.solidcore.com.

—Jeff James

InstantDoc ID 96726

NETIKUS.NET EventSentry 2.8

Editor's Note: To read the full-length version of this review, go to http://www.windowsitpro.com and enter InstantDoc ID 96770.

NETIKUS.NET's EventSentry 2.8 is an excellent event-log and system-health monitoring and consolidation tool. Operating under Windows Server 2003, XP, 2000, and NT (including x64 versions), EventSentry offers a broad complement of filtering, alerting, and Web-based reporting options. Optionally, you can use EventSentry to consolidate monitored logs to an ODBC database, and the installation routines provide explicit support for Microsoft SQL Server, MySQL, and Access.

SUMMARY

NETIKUS.NET EventSentry 2.8

PROS: Broad feature set, including system health monitoring, support for custom event logs, and Syslog monitoring; easy-to-use console for configuring filters, actions, and monitoring

CONS: Remote administration lacks full access to the configuration created at another console; reporting could be more sophisticated; publishing options are few

RATING: ◆◆◆◆◆

PRICE: Full license starts at $75 per monitored host; Syslog- or heartbeat-only licenses start at 10 hosts for $79.

RECOMMENDATION: EventSentry offers terrific log- and health-monitoring tools at a very reasonable price, and gets my strong recommendation.

CONTACT: NETIKUS.NET • http://www.netikus.net • 877-638-4587 or 312-624-7698

By all rights, EventSentry should have been included in my recent comparative review, "Log Management Products for SMBs" (InstantDoc ID 95955)—a simple oversight. Considering EventSentry's comprehensive feature set and ease of use, the tool would have stood in the top tier.

EventSentry is comprised of four key components: a management console, the EventSentry agent, the heartbeat agent, and Web-reporting components. The EventSentry agent runs as a service, monitoring event logs and system health. The heartbeat agent monitors the uptime of remote hosts and EventSentry agents. ASP-based Web reports let you easily view the information that EventSentry collects: logs and alerts, as well as system health.

I installed EventSentry on a Windows 2003 system. EventSentry's management console is logically organized, with a console tree structure on the left and a details pane on the right. Although you can install the management console GUI on multiple systems, it doesn't support full remote administration. You can't install agents or push out configuration changes from a remote-console connection.

EventSentry supports 14 distinct types of actions, including writing to a database, a text file or a syslog server; notifying via email, network send, SNMP, or pager; shutting down the system; and changing the status of a service. I created actions to write to a SQL Server database, notify via email, and play a sound file. EventSentry offers a variety of predefined filter groups, and I found it easy to create additional filters and filter groups, and to define custom event logs.

Assigning an action to each filter in a package, or to the package as a whole, is quite convenient. Similarly, your ability to organize monitored computers within named groups lets you deploy and update both the EventSentry agent and client configurations to groups of computers at once. Right-clicking a computer or group displays a list of all filter packages, letting you select a check box to choose those you want to assign.

Event Sentry offers a collection of filter packages devoted to system-health and performance monitoring. You can set monitoring intervals and thresholds for notification, and you can assign to the filters and groups the same set of actions valid for event log filters.

EventSentry boasts a comprehensive set of monitoring, recording, and alerting options—although I would welcome enhancements to the reporting and remote-console features. A breeze to learn and use, throwing few surprises my way, EventSentry nevertheless gains my recommendation: Consider it closely for your environment.

—John Green

InstantDoc ID 96770

Paul's Picks

Summaries of in-depth product reviews on Paul Thurrott's SuperSite for Windows

http://www.winsupersite.com

Apple iPhone

PROS: Cutting-edge technology, great battery life.

CONS: Not a managed smart phone, no true Microsoft Exchange compatibility.

RATING: ◆◆◆◇◇

RECOMMENDATION: Apple's iPhone arrived amidst an explosion of hype and consumer excitement, and while the device's technology lives up to the advance billing, this isn't a smart phone for most businesses. The iPhone lacks true Exchange compatibility, can't be centrally managed, and doesn't include the types of smart phone features that today's Windows Mobile and RIM Blackberry users expect. For now, corporations should avoid the iPhone and stick with more traditional smart phone solutions.

CONTACT: Apple • 408-996-1010 • http://www.apple.com

DISCUSSION: http://www.winsupersite.com/reviews/winlive_hotmail_02.asp

Microsoft Windows Live OneCare 2.0

PROS: "Admin-in-a-box" for small and home businesses, brings Vista features to Windows XP, multi-PC management.

CONS: Not a true enterprise product, aimed only at the smallest businesses.

RATING: ◆◆◆◇◇

RECOMMENDATION: Small businesses should look at Windows Live OneCare very closely because of its low price and excellent security and PC management features. OneCare 2.0 adds functionality that makes this product more appropriate for small businesses, including multi-PC management with monthly reporting, automatic printer sharing, and proactive PC health fixes and recommendations. But the best features might be those that bring Windows Vista functionality to XP users.

CONTACT: Microsoft • 800-426-9400 • http://www.microsoft.com

DISCUSSION: http://www.winsupersite.com/reviews/winlive_hotmail_02.asp

InstantDoc ID 96773

Your potential. Our passion.®

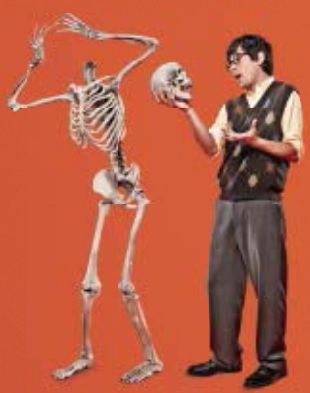
Microsoft®

defeating skeletons. easy.

1. Pinch yourself.
You're being chased down a long, dark hall. Only the hall leads to the lunch room and it's no nightmare; Skeletons really have attacked your office. Put aside fear and face the task at hand.

2. Sneak up and scare them.
Skeletons love scaring people, but why? Anyone that obsessed with scaring others is probably scared themselves. But of what? A psychologist might say the Skeletons fear exposure, for who is more exposed? Any psychologists out there?

3. Use nondairy creamer.
Drinking milk builds strong bones. And a good calcium supplement is a must for women over 50, when the risk of osteoporosis can increase dramatically. Deny the Skeletons this key nutrient, you'll see them weaken and crumble.



4. Put on a show.
It's a classic scene. Hamlet, the melancholy Dane, finds the skull of Yorick in the graveyard, and muses on the inevitability of death. This is a big role for a Skeleton—use it as bait. Offer him the part, and simply keep the prop.

5. Destroy the dark crystal.
What unholy force animates the Skeletons? Has the fabled dark crystal of Fabrikam fallen into the hands of an enemy? Find the crystal at all costs, fling it into the fiery river at the heart of Bone Mountain, then sell the movie rights.

defeating viruses. easier.

1. Implement Microsoft Forefront.
Forefront™ makes defending your systems easier. It's a simple-to-use, integrated family of client, server, and edge security products (such as Forefront Client Security) that helps you stay ahead of your security threats more easily than ever. For case studies, free trials, demos, and all the latest moves, visit **easyeasier.com**

Microsoft®
Forefront™

BY TONY PILTZECKER

MICROSOFT OFFICE COMMUNICATIONS SERVER 2007

Beta 3 is a step toward truly unified communications

If you haven't yet heard about Microsoft's Unified Communications (UC) strategy, chances are good that you'll be hearing about it *ad nauseam* over the next 6 to 12 months. Steve Ballmer and his crew have made it very clear that they're ready to take the world of convergence head-on. With apologies to Microsoft Speech Server, Exchange Server 2007 Unified Messaging (UM)—released late last year—was Microsoft's first real attempt to enter the IP telephony market. Exchange UM provides the ability to integrate voicemail, fax, and of course email into a single mailbox solution. However, Exchange UM still relies on third-party telephony systems, whether legacy PBX or IP-PBX solutions.

At the same time, the concept of "presence" is causing quite a stir. Companies such as Microsoft, Cisco, and IBM are all battling for the rights to own and control the presence engine. What is presence? It's the ability to locate and identify a person (or group of people) and communicate with them, regardless of the means of communication (e.g., PC, desk phone, cell phone, IM). Microsoft's first attempt at presence was Microsoft Office Live Communications Server 2005 (LCS 2005). (Exchange 2000 Server IM and LCS 2003 predate LCS 2005 but were crude at best.) However, LCS wasn't an ideal solution.

With the introduction of Microsoft Office Communications Server (OCS) 2007, Microsoft merges call control (the ability to route and place a telephone call) and presence technologies together into a single offering. OCS 2007 Beta 3 was released in March 2007. Since the product's release, Microsoft has been very proactive in distributing the various deployment and administration guides, as well as providing hands-on training for many of their key partners.

Although I've been through Microsoft's official "Ignite" program for partners, I wanted to step outside the Microsoft sandbox and install OCS Beta 3 from scratch in my environment. To test the product's functionality, I needed several puzzle pieces: Active Directory (AD), Exchange 2007, a member server for OCS, and a Session Initiation Protocol–Public Switched Telephone Network (SIP-PSTN) gateway. I used an inexpensive, yet very configurable, gateway device from AudioCodes—the MP-114 (http://www.audiocodes.com/content.aspx?voip=2823).

Installation

Because AD will contain all of the SIP user information and settings, you need to extend the schema to accommodate these additional attributes. The schema extension itself is fairly straightforward, with the same administrative requirements as Exchange, LCS, and Microsoft Systems Management Server (SMS).

ILLUSTRATION BY ZOO IMAGES / IMAGES.COM

The Essential Guide to

October 2007

EXCHANGE 2007 Storage Planning & Implementation

by Paul Robichaux
and Devin Ganger

Special Advertising Supplement
Sponsored by
DELL™

As you prepare to transition to Exchange 2007, you'll find that there are several areas of design and implementation that require a different perspective from previous versions. Storage design is one of these areas; the architectural changes in Exchange 2007 mean that you'll need to approach your Exchange environment with a fresh eye to design the optimum Exchange infrastructure for your needs. The major changes in Exchange 2007 include Microsoft's move to a 64-bit architecture, new server roles, changes to the way that the Extensible Storage Engine (ESE) stores and formats data, and new options for data protection and high availability. In this guide, I'll explore these changes and explain what impact they'll have on your Exchange 2007 storage planning and implementation.

Exchange 2007 Storage Architecture

Microsoft's decision to require 64-bit hardware and 64-bit versions of Windows for Exchange 2007 has some far-reaching effects. The biggest effect from a storage point of view is actually provided by the operating system: 64-bit servers running a 64-bit edition of Windows Server can handle much more physical RAM than 32-bit servers. Increasing the amount of supported RAM benefits Exchange in two important ways: caching and kernel memory pools.

Improved Caching

While the Exchange ESE implementation has always supported caches, in Exchange 2003 this cache was limited in size to 1GB. That sounds like a lot of RAM, but the fact is that the more pages ESE can cache, the less it will have to hit the disk. By requiring 64-bit Windows and servers, Exchange 2007 can effectively take advantage of this additional RAM to cache more mailbox database pages in memory.

The selection of which pages to cache is an important part of the Exchange 2007 caching strategy. Microsoft determined that caching would provide the most benefit to data that you can expect most or all of your users to access – the contents of their Inboxes and other default folders. Because of this, Exchange tries to maximize the impact of caching by loading the common datasets from all of the mailboxes on the server into the cache. This permits common data access requests to be served from the cache, rather than requiring a separate I/O request.

Larger Kernel Memory Pools

The 64-bit editions of Windows also provide a second benefit to Exchange. Under 32-bit Windows, there was a physical maximum of 4GB of RAM; this total amount had to be split between the Windows kernel and applications such as Exchange. By default, this was divided evenly: 2GB for the kernel, 2GB for applications. On dedicated Exchange mailbox servers, it was a common practice to use the /3GB switch to change this allocation: 1GB for the kernel, 3GB for Exchange. While this configuration was good for the Exchange process (even if it couldn't expand the cache), it had a corresponding price.

The kernel maintains two memory pools, the page memory pool and the non-paged memory pool, that are used by various components of the system. Drivers for the HBA interfaces common with many SAN systems required space in these pools, as did each MAPI RPC connection to the Exchange information store. With a top end of physical RAM, decreasing the amount of RAM for the kernel placed a hard limit on the number of simultaneous connections 32-bit Exchange servers could support before the kernel memory pools were exhausted.

Reduced I/O

Microsoft originally claimed a potential reduction of up to 70 percent in the number of I/O operations per second (IOPS) required. As you might expect, real-world figures for live deployments show that number to be a bit optimistic; in order to match that level of performance in your real-world deployment, your mailbox servers have to be designed with some very stringent requirements in mind, such as the following:

- Your users will all need to be upgraded to Outlook 2007 in order to take advantage of the latest bandwidth optimizations that have been introduced. Older clients are not quite as efficient.
- You will need most, if not all, of your users to be running Outlook in cached mode; this helps consolidate read and write operations against mailboxes and increases the usefulness of caching.
- You will need to minimize the number of simultaneous connections to each mailbox. Laptops, Outlook Web Access, and mobile devices can all increase or even multiply the amount of traffic to each mailbox.

However, it remains true that buying large amounts of RAM for a server is almost always cheaper than buying additional SAN capacity, which means that you can still achieve impressive I/O reductions in your own environment

For example, consider the cost of upgrading an existing 64-bit-capable server that now has 4GB of RAM; an additional 4GB of RAM costs about $100 per GB. However, adding it can increase Exchange 2007's caching and reduce the number of IOPS required to support the same number of users on the same computer by up to 40%. You would need to add far more hard drives in order to gain the same performance benefit, at considerably more cost.

Better Use of Resources

Due to the nature of Exchange I/O, storage subsystems usually require far more hard drives to satisfy the number of spindles and IOPS load than would be required to meet the basic storage capacity. This is because in the past decade of hard drive technology, capacity has increased far more rapidly than access times; Exchange 2003 was developed when 9GB and 18GB SCSI disks were the high-end options and was designed with their characteristics in mind. As a result, most existing Exchange storage designs have spare drive capacity, due to the large drives in modern arrays.

The reduction of I/O requirements in Exchange 2007 means that you can do one of two things with this capacity:

- First, you can host more mailboxes on the same hardware. Exchange 2007 continues the trend in server consolidation that was started in previous versions. Exchange 2007 mailbox servers that are using storage systems designed against Exchange 2003 can make use of this additional disk capacity to store additional mailboxes; these mailboxes will also be cached, reducing the impact they have on the overall system I/O. Even on a new storage system, Exchange 2007 takes better advantage of the modern high-capacity drives sold in today's market.
- Second, you can host larger mailboxes on the same hardware. Allowing your users to store more mail data in their mailboxes usually has less of an impact on the total system performance than you might think. When your users are allowed to packrat more data, few of them actually access that additional data regularly. It just sits there on the hard drive most of the time. By increasing mailbox size, you're using the storage capacity of modern hard drives to better benefit and giving your users better access to their data.

If you're feeling bold, you can even do both at once: put more mailboxes on a single server and increase the size of those mailboxes. In Exchange 2007 Standard Edition, you can create a total of five mailbox databases; however, each of them can be in their own storage group. In Enterprise Edition, you have up to 50 databases, each of which can also have a separate storage group. Microsoft recommends that you follow this one-to-one allocation of storage groups and databases in order to gain the benefits of having a separate set of transaction logs for each database. This allows you to increase your mailbox database size without affecting your ability to meet your backup and restore SLAs for each of your databases.

Measuring Exchange 2007 Storage Performance

For some time, Microsoft has been shipping a tool called the Exchange Load Simulator, or just Loadsim. Loadsim's purpose in life is to simulate the amount of load created by a specified mix of MAPI clients; the Loadsim engine uses a tailored mix of MAPI operations to simulate the behavior of hundreds of users at once. While it's a useful tool, it doesn't accurately predict the load patterns created by Outlook 2007 and Exchange 2007, and it's very resource-intensive.

Loadgen

To fix this, Microsoft wrote a brand-new tool, the Exchange Load Generator (also known as "Loadgen" and formerly code-named Swordfish). Loadgen can run in two modes: in stress mode, it attempts to drive as much load to the target servers as possible. In normal mode, it follows the usage profile that you set, which is pretty comprehensive. Apart from setting the number of users and the average mailbox sizes that you want to simulate, you can also control things like how often a generated message will contain an attachment, the average number of calendar items that a simulated user creates per day, and the percentage of delivered messages that should be deleted. This is a departure from Loadsim, which essentially restricted you to using "heavy," "medium," or "light" users. Loadgen has another extremely useful feature: you can use it to test multiple Exchange servers at once, giving you a meaningful way to simulate complex multi-server networks to see whether they can handle the expected load.

The most effective way to use Loadgen is to set up an Exchange 2007 server in your proposed configuration, then use Windows' Performance Monitor to gather real load data for your existing servers. That way, you can see how busy your server is, how many IOPS it generates, and so on. Once you have that baseline performance data, you can run Loadgen and record the results from a default configuration to see where the differences are. Next, tweak the Loadgen profiles to most closely match the actual observed behavior from your server, then, as necessary, adjust your Exchange 2007 configuration for the number of users and mailboxes you expect it to handle.

Jetstress

There's another tool you should know about, too: Jetstress. While Loadgen is designed to allow you to simulate real-world loads on your Exchange infrastructure, Jetstress is designed to do just one thing: beat up on the Exchange information store and make it bleed. By using Jetstress, you can validate through hard experience the highest amount of performance that your Exchange design can handle and ensure that it meets the highest amount of load you expect to see, not just your daily amount of load. Sure, your mailbox servers can handle the load at 5 pm on Friday, but can they handle the shock of 8 am Monday when everyone is first logging onto their mailboxes for the week? If so, how much spare capacity do you have; is it enough to handle a drive failure that throws a critical array into degraded mode? With Jetstress, you'll know.

Jetstress 2007 has been improved; the GUI has been simplified and looks more like the other Exchange management tools and analyzers. While it includes built-in reporting, you should use it in conjunction with Performance Monitor to capture detailed results for your later analysis. Jetstress is intended to be run on the combination of your server hardware and Windows, before you have installed Exchange but after you have configured your storage options such as direct attach storage (DAS) volumes and SAN LUNs. It uses the same ESE libraries used in Exchange to test the disk and cache performance of your server and storage configuration, allowing you to validate your hardware design before actually taking the irrevocable steps of updating your Active Directory schema and installing Exchange 2007 into your organization.

Sizing Exchange 2007 Storage

Properly designing the storage system you need for your Exchange 2007 deployment is an iterative process. With past versions of Exchange, supporting a high IOPS load on an Exchange mailbox server practically condemned you to the cost and administrative overhead of a high-end SAN or iSCSI SAN system. One of the design goals of Exchange 2007 is to allow you the use of DAS options under a much larger number of circumstances.

So how do you know which to use? As you might imagine, there are a number of factors to consider:

- If you are planning on using traditional failover clustering, now named Shared Copy Clustering (SCC), you must have a shared storage system between all of the nodes in your cluster. Some DAS solutions (such as the Dell MD3000) can accommodate two-node clusters; however, larger clusters will require a SAN solution so that all of the mailbox server nodes have access to the storage groups and mailbox databases in a failover.
- If you are planning on using the new Continuous Clustered Replication (CCR) feature, your two mailbox nodes require the Microsoft Clustering Service. However, CCR uses database replication rather than a shared copy, so you have a choice of whether to use DAS or a SAN. If you have an existing SAN that you want to use, each node should have its own LUNs, not shared copies of the databases and storage groups; CCR nodes won't fail over disk resources.
- If you are planning on using the Local Continuous Replication (LCR) feature, you should probably consider the use of DAS, at least for the second copy of your LCR-protected mailbox databases. LCR is designed to provide a second copy of the databases on the local system to guard against storage failures. You could use multiple SAN LUNs for this purpose, but that probably doesn't make a lot of sense in most environments.
- Do you have the required number of drive spindles in your SAN to accommodate the IOPS load of your Exchange server? Many SAN administrators and vendors do not understand the specialized character of Exchange I/O patterns and attempt to meet the space requirements without providing an adequate number of spindles. Others see the "wasted" space of Exchange LUNs and try to share that space with other data sources such as SQL Server – often with catastrophic effects on your Exchange server performance.

You can often find expert help for your Exchange storage design process by consulting with hardware vendors who understand how to design for Exchange. Many vendors even offer online or computerized calculators; you feed in the parameters for your system, such as type of user load, number of mailboxes, and required configurations and features, and in return receive recommendations for the specific server and storage systems you need to buy. Dell makes their Exchange 2007 Advisor available from their Web site, allowing you to start your design process there and look at the characteristics of the hardware options it recommends. You can find the Dell Exchange 2007 Advisor at http://www.dell.com/content/topics/global.aspx/tools/advisors/exchange_advisor?c=us&cs=555&l=en&s=biz

Conclusion

Planning your Exchange storage configuration has gotten easier with Exchange 2007, thanks to the performance benefits Microsoft has gained by moving to a 64-bit architecture. The improved caching and use of kernel memory allow you to host larger mailboxes or more mailboxes per server with reduced I/O requirements, and the Loadgen and Jetstress tools give you the means to test your configuration with confidence. Exchange 2007's performance gains allow you to make use of DAS in more scenarios, reducing the costs associated with SAN storage systems.

Paul Robichaux is a founding partner for 3sharp, an MCSE, and an Exchange MVP. He is the author of several books, including *The Exchange Server Cookbook* (O'Reilly and Associates), and creator of the http://www.exchangefaq.org Web site.

Devin Ganger is a messaging architect for 3sharp, an Exchange MVP, and co-author of *The Exchange Server Cookbook* (O'Reilly and Associates).

Likewise, OCS setup must be run at both the forest level and domain level to prep AD. Microsoft has made this portion of the setup process almost foolproof by reducing the number of use-interactive steps required, as well as preventing you from being able to initiate a step without finishing the earlier steps.

If you're familiar with LCS installation, you'll be happy to know that Microsoft has simplified the process of installing certificates as well. However, a glitch I stumbled upon is that if your forest and domain functional levels aren't set for Windows Server 2003, the certificate requests will fail with very little explanation.

One of the handiest installation features is the verification process, which lets you verify not only server configuration but also connectivity. I discuss installation of the other server roles later in the article.

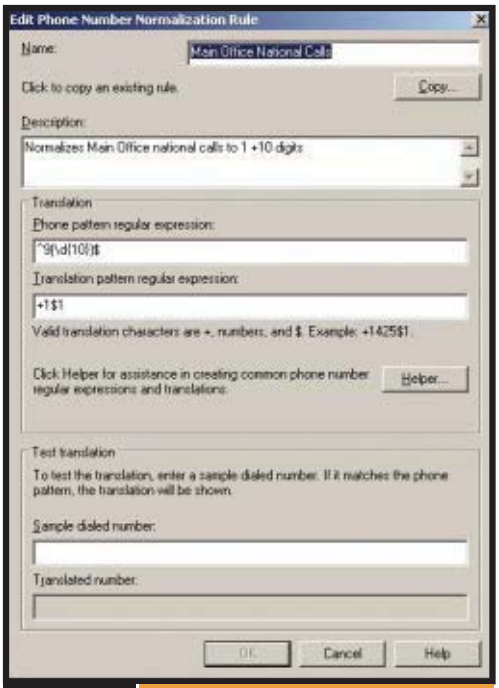


Figure 1: Editing a phone number normalization rule

Configuration

For anyone familiar with AD, enabling and configuring OCS users is easy. You can enable users in bulk or on a user-by-user basis. The minimum setting that must be completed is the SIP address assignment (commonly, the user's email address). However, additional settings can be configured, including federation (presence connectivity with other LCS/OCS-enabled companies), public IM connectivity (Yahoo!, MSN, AOL), and remote user access (the ability to connect to OCS from outside the firewall).

One of OCS's new features is Enhanced Presence, which you can also configure on a per-user basis. Enhanced Presence lets you place users into various Presence Access Levels (Block, Public, Workplace, Team Members, and Personal). Each level, from left to right, allows more presence data to be presented to contacts. For example, contacts who are in the Public level can see only Presence State (e.g., Online, Busy), Display Name, E-mail Address, Title, and Company. At the other end of the spectrum, Personal contacts can essentially see all user data stored in AD for a particular user (e.g., Work Phone, Home Phone). A caveat with Enhanced Presence is that if you enable it, users *must* use Microsoft Office Communicator (MOC) 2007. Older versions (e.g., Windows Live Messenger, MOC 2005) won't be able to connect.

With relation to OCS itself, most of the configuration is already complete in this scenario. The only piece that still needs configuration is DNS. OCS, like LCS, requires the creation of specific SRV records in order for automatic server detection to function. Within DNS, you must create an "Other New Record," setting the Service type to _sipinternaltls, protocol to _tcp, and port number to 5061 (which represents Transport Layer Security—TLS—encrypted SIP traffic). After configuration, users won't need to enter a specific OCS server IP address or Fully Qualified Domain Name (FQDN) address into the MOC client. This is especially important for users who work both onsite and remotely, because the two IP addresses will almost certainly vary.

SUMMARY

Microsoft Office Communications Server 2007 Beta 3

PROS: Easy setup and installation; improved presence capabilities over LCS 2005

CONS: Administration and scalability features need improvement before release to manufacturing (RTM)

RECOMMENDATION: OCS 2007's combined presence, collaboration, voice, video, and conferencing features make it a one-stop UC solution.

CONTACT: Microsoft • http://office.microsoft.com/en-us/communicationsserver/default.aspx

Additional Roles

Microsoft seems to be moving toward a distributed solution model in which a single product needs to be installed on separate physical servers. Such is the case in Exchange 2007, Microsoft System Center Operations Manager 2007, and now OCS 2007. What this requirement actually means depends on the size of your implementation. Roles can be consolidated onto one piece of hardware, but for larger organizations that will be taxing the resources on an OCS server, additional physical hardware is needed. The two roles that carry over from LCS 2005 are Access Proxy and Director.

The Access Proxy role lets you enable remote connectivity, federation, and public IM connectivity. Although this role is fairly straightforward, additional network planning is necessary because it resides in a demilitarized zone (DMZ).

The Director role is used to route traffic to the proper OCS pool (OCS servers), as well as act as a middleman between the Access Proxy role and the front-end OCS servers. A compromised Access Proxy role can't bring down AD or the OCS front-end servers, because the Director role would take the brunt of any Denial of Service (DoS) attack. Installing the Director role is simple.

OCS 2007 also includes four new roles. These roles are telephony enablement (Mediation Server), on-premise conferencing (Microsoft Office Live Meeting), compliance (Archiving Server), and remote telephony (Edge Server).

Telephony configuration. Telephony is particularly interesting to me because of what my company does, so I've spent quite a bit of time working with OCS's telephony features. Installing and configuring OCS's Mediation Server role is far simpler than installing some of the more traditional (if we can use that word yet) VoIP vendor solutions. Because AD already contains much of the necessary user information, the only areas you need to focus on are call routing and rules. Setting rules can be a bit confusing if you don't have any experience writing regular expressions. Figure 1 shows an example. The Help files are almost nonexistent in OCS Beta 3. However, searching the Web can be useful.

After you've written your rules (and configured your SIP gateway), you can begin testing the OCS softphone (which is the MOC 2007 application) connectivity to the outside world. In my lab, I used an AudioCodes MP-114 device (with a plain old telephone), as well as an SIP trunk to my Cisco CallManager 5 server. If you don't have access to such equipment, you can use MOC, which also functions as a softphone, to make MOC-to-MOC calls as if they were telephony calls. This process effectively eliminates the need for a traditional handset in order to place a phone call. Microsoft recently announced that their handset line is in full production via several manufacturing partners (http://www.microsoft.com/presspass/press/2007/may07/05-13newgenworkphonespr.mspx), which will present some interesting solutions as well.

Something that I found perplexing, at least in the beta version of OCS, is that only one PSTN gateway is allowed per Mediation Server role. Depending on the size of the environment, it's not unreasonable to assume that a company might have one gateway supporting its T1 links and another gateway supporting PSTN, or possibly a split load for redundancy. We can only hope that this deficiency is addressed before release.

On a similar note, although OCS's Exchange 2007 UM tie-in appears to be pretty tight, some of the steps for integrating the two aren't as seamless as you'd expect. For instance, you must run several command-line scripts, as well as stop and start several services, for OCS and Exchange 2007 UM to communicate and interoperate.

Conferencing. For many years now, Microsoft has offered hosted Live Meeting services via the Web. With the introduction of OCS 2007, Microsoft brings that same functionality on-premise. OCS 2007 lets you provide ad-hoc escalation of conferences (e.g., via IM) for internal and federated contacts, as well as scheduled Live Meeting conferences for "trusted" and anonymous contacts. Thus, many of the meeting events that you previously outsourced to Microsoft or other companies (e.g., WebEx) can now be maintained inside your network. In addition, an Outlook plug-in lets you use Outlook's familiar scheduling interface to set up conferences.

The Live Meeting role's configuration is straightforward and mostly focused on meeting policies—particularly who is allowed to participate. The Live Meeting user plug-ins are hands-off, requiring only the basic user information (sign-in name, service URL, and credentials), as well as a complete restart of Outlook. OCS 2007's on-premise conferencing services will be a cost-effective, user-friendly solution for companies. Oddly enough, OCS 2007 is becoming available at the same time that Cisco is moving in the other direction—from on-premise (Cisco MeetingPlace) to off-premise (with the acquisition of WebEx). Only time will tell which method end users prefer, or whether both methods will simply coexist.

Compliance. One of the major reasons for implementing an in-house presence solution is to keep confidential company information off the public wire. However, because you can configure OCS for federation and public IM connectivity, this information can be leaked. Although actually preventing users from revealing this type of information is difficult, you can easily record and audit communications that initiated from OCS.

One of the downsides of archiving for many companies is that to implement archiving, you typically need another server, as well as another instance of Microsoft SQL Server. However, installing the archiving service is a straightforward process. The last step in configuration is simply associating the Archiving Server role with a front-end server. Again, stopping and restarting OCS services on the front-end servers is a bit disruptive but is necessary to properly configure the archiving server.

Viewing archived OCS data is no easy feat for a SQL Server novice. The only way I could find to view an archived conversation was through SQL Server Management Studio (SSMS)—and only then because of some documentation that Microsoft provided to me.

A new OCS feature, Call Detail Record (CDR), includes some slick trending and analysis reports that take advantage of Excel 2007's new conditional formatting feature. CDR isn't new to telephony—this feature is crucial to a telephony system's reliability and functionality. In addition to standard CDR information (e.g., missed calls, call duration), OCS's CDR reports provide several key pieces of information, including tracking of:

- application sharing sessions
- A/V sessions
- file transfer sessions
- length of IM sessions
- number of IM sessions
- number of IM messages
- number of IM users
- remote access sessions

Remote telephony. In LCS 2005, if you want to work remotely and use A/V, data sharing, or remote access, you must first connect through your VPN. This requirement is necessary because these features are intended to be point-to-point, and they can't be proxied via the LCS 2005 Access Proxy. Because public IM services already provided these functions, improving upon this area was important when Microsoft replaced LCS 2005 with OCS 2007. However, you still need yet another edge server. Whether the Edge Server role can (or will) coexist with LCS 2005's Access Proxy server role is yet to be determined—but it must if you want to provide Live Meeting, A/V, or telephony support for remote users.

If connectivity "at the edge" works as intended, the Edge Server role will be a major victory for Microsoft. One area that will become clear over time is how the quality of a call that's routed through the Internet via the edge server is affected, especially when multiple users are hitting the gateway at once. According to Microsoft, a high-quality two-way (dual stream) call requires approximately 80Kbps of bandwidth. Multiply that by 20 simultaneous calls, and you could have some congestion on your Internet pipe.

A Force to Be Reckoned With

When Microsoft releases it, OCS 2007 will be a force to be reckoned with. The previous LCS presence capabilities have been greatly improved, and the voice capabilities have a lot of promise. Although certain features still need improvement from the beta version (mainly related to administration and scalability), OCS 2007's one-stop-shopping approach to presence, collaboration, voice, video, and conferencing will make the product more of a "need" than a "want." With OCS 2007, Microsoft deftly reigns in the current silos of communication, putting the rest of the UC world on notice.

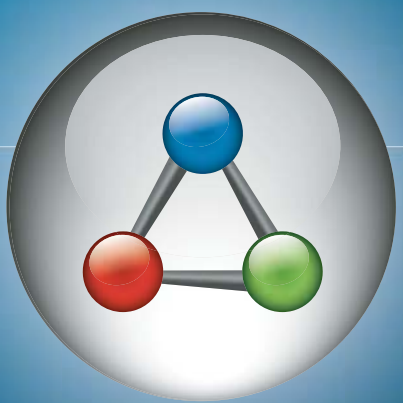
InstantDoc ID 96826

Tony Piltzecker
(tony@uccentral.com) is an independent IT consultant based in Boston. He has been an author and technical editor for several IT-related publications and has worked in IT for more than a decade.

busi·ness
pro·cess
au·to·ma·tion

[biz-nis | pros-es | aw-tuh-mey-shuhn]

The replacement of a manual business process with an automated one, usually through the use of **advanced technologies**.



AutoMate BPA Server 7™

The Business Process Automation Server from Network Automation

NO CODE, NO LIMITS

Automates business & IT processes
Eliminates the need for job schedulers, scripts & batch files
Intuitive drag-and-drop workflow design & task development

Visit **WhatIsBPAServer.com** to learn more about **BPA Server 7** and how the world leader in **Business Process Automation** is advancing the field. Again.

NETWORK AUTOMATION

www.WhatIsBPAServer.com
888-786-4796

Redmond MVP Most Valuable Product

Windows IT Pro READERS CHOICE 2006 Winner

Windows IT Pro EDITOR'S BEST 2007 WINNER

Uncontrolled use of USB sticks, MP3 players and PDAs opens up your network to data theft and viruses

Control user access to all devices connected to your network with GFI EndPointSecurity

GFI EndPointSecurity

TMC LABS INNOVATION 2006 AWARD

Window Security.com Gold Award ★★★★

You have invested in network anti-virus software, firewalls, email and web content security to protect against external threats. Yet any user can come into the office, plug in a USB stick and take in/out over 32 GB of data. Users can take confidential data or they can unknowingly introduce viruses, trojans, illegal software and more – actions that can affect your network and company severely. Yet, as an administrator you had no way to control this until now!

GFI EndPointSecurity allows administrators to centrally manage user access to devices such as iPods, USB sticks, PDAs, laptops and more. Controlling user access to such connectable devices allows you to:

- Protect your network by ensuring users don't introduce viruses and other malware
- Stop the alarming rate of insider data theft
- Increase employee productivity by preventing them from bringing other work, games or personal projects to their workplace
- Prevent users from introducing illegal or unauthorized software on their machines.

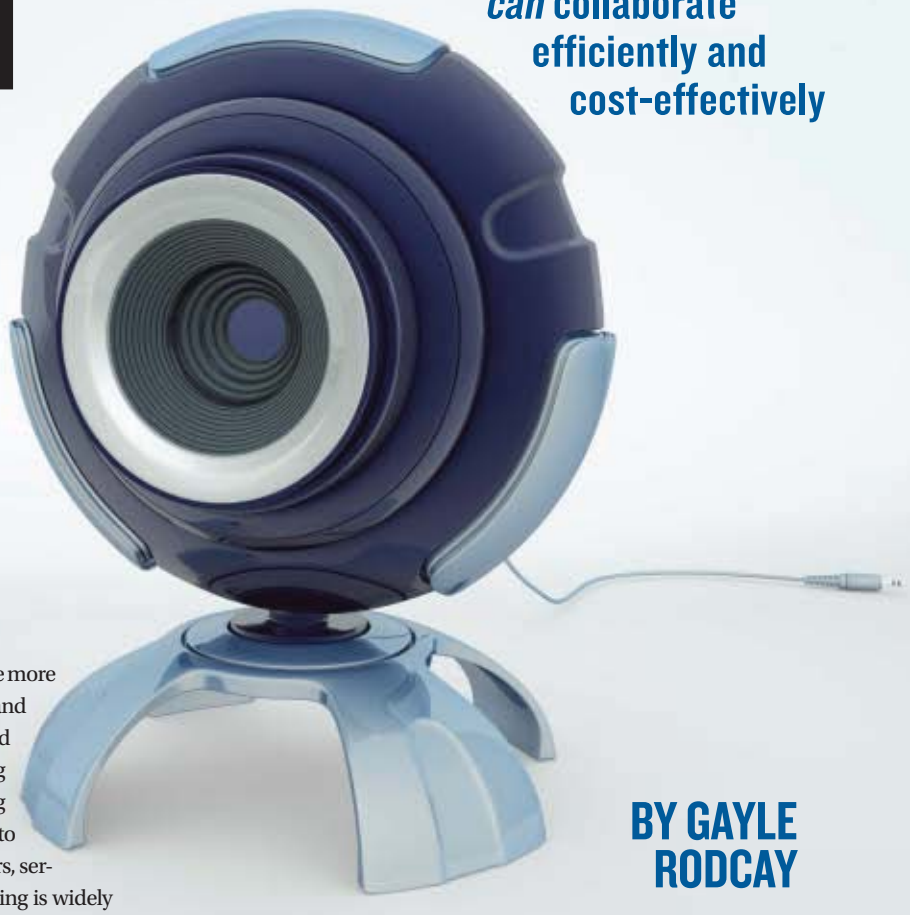
Download your FREE trial version from www.gfi.com/esw/

GFI NETWORK SECURITY
CONTENT SECURITY
MESSAGING

tel: +1 888 243 4329 | fax: +1 919 379 3402 | email: sales@gfiusa.com | url: www.gfi.com/esw/

MEET ME ON THE WEB

A distributed global work force *can* collaborate efficiently and cost-effectively



BY GAYLE RODCAY

As enterprises grow and partners and employees become more dispersed and mobile, maintaining communication and collaboration becomes increasingly important—and difficult. Meanwhile, travel and off-site meetings are falling victim to cost cutting. In this landscape, remote conferencing tools break down geographic barriers and allow companies to more easily and inexpensively connect with partners, vendors, service providers, customers, and employees. Audio conferencing is widely used today, but more and more businesses are discovering the additional advantages offered by Web-conferencing solutions.

Although the Web-conferencing market is still young, recent acquisitions by **Cisco Systems** (of WebEx Communications) and **Adobe Systems** (of Macromedia Breeze) indicate that it's already beginning to consolidate. But a dizzying array of deployment and pricing models, integrated services, and collaboration features continue to make it difficult for businesses to settle on a viable long-term solution.

Service or Software?

Web-conferencing solutions are available either as a hosted service (i.e., Software as a Service—SaaS) or as a purchased technology that you install in-house. To decide between the two and achieve the best ROI, organizations need to consider the number of employees who will use the solution, the number of concurrent seat licenses needed, and how much time is spent in conferences.

With SaaS, up-front expenses are nonexistent or minimal, there is no charge for upgrades or new features, and companies aren't locked into a particular software. SaaS solutions typically charge either a per-user, per-minute fee or a flat-rate, unlimited-use fee for a specified amount of time. Small-to-midsized businesses with low usage levels and companies that are evaluating conferencing solutions are likely better off with a hosted service.

Purchasing Web-conferencing technology and equipment is usually the way to go for companies that have high usage levels. Up-front costs are significant, but over time, companies avoid the spiraling usage costs of SaaS. In-house solutions offer more control over application performance, availability, and—because the application is installed inside the organization's firewall—security. Further, organizations that want to integrate their conferencing solution with crucial business applications, such as customer relationship management, ERP, information management, and project management, will find that managing the integration is easier if they have an in-house solution. Although recent **Gartner** research shows that 70 percent to 80 percent of Web conferences use SaaS, Gartner expects that percentage to drop in favor of more on-site solutions because of cost, reliability, and security concerns.

Quite a few vendors make their Web-conferencing solutions available both as a hosted service and as standalone software, letting companies choose the model that best suits their needs. Microsoft, for one, will offer a hosted model for its Microsoft Office Live Meeting 2007 (which is due to ship this fall) as well as a standalone solution, which

will be marketed as Microsoft Office Communications Server 2007. Cisco's WebEx Meeting Center and Adobe Acrobat Connect (formerly Macromedia Breeze Meeting Center) are also available in both forms. And **Interwise** offers not only hosted-service and standalone versions of its Interwise Connect product, but also a hybrid solution that lets you seamlessly fail over to the host-based version should your in-house application fail, and vice versa.

Some Web-conferencing providers offer a pay-as-you-go option. This no-subscription, no-seat-license, no-minimum-usage-fee plan is an attractive alternative for small businesses or organizations that conduct few online meetings. Examples include the **Meeting On Now** service, which lets you reserve a "meeting room" for $12.50 per day, and **Unlimited Conferencing**, which offers a pay-as-you-go service for 14.9 cents per minute per participant.

Virtually Speaking

Most organizations begin looking at Web conferencing when their needs expand beyond the capabilities of their voice-conferencing system. Companies that simply want to add Web conferencing functionality to their telephone conferencing system can contract with a service provider to add the Web component to their existing audio conferencing solution. Another option is to connect a purchased in-house Web-conferencing application to the corporate phone system, which adds voice capabilities. **Sonexis** ConferenceManager offers a twist on this model: an audio-conferencing bridge with built-in plug-and-play Web-conferencing capabilities.

Increasingly, solution providers are integrating audio with Web conferencing, giving users a choice of audio-only conferencing or integrated audio and Web conferencing. For example, **Citrix Online**'s Citrix GoToMeeting includes a conference call service, which provides a phone number that meeting participants can dial to join the conference. Participants are charged their standard long-distance rate for the call.

VoIP is also becoming more widespread in conferencing solutions. In addition to its low cost, VoIP lets participants listen over a phone or directly through their computer, depending on the service and equipment used. Solutions that provide audio conferencing via both VoIP and telephone allow users who don't have Internet access to participate in meetings, even though they can't see any online content. (They could, however, work with an offline Microsoft PowerPoint presentation.) Adobe Acrobat Connect, Live Meeting 2007, **Elluminate** Live!, **eBLVD** Online Meetings, Interwise Connect, and WebEx Meeting Center all offer both traditional voice communication and VoIP. Such solutions let users switch from telephone to VoIP at any time. For example, attendees who join a meeting while away from the office can switch to another phone or VoIP when they return to their desk. Unless your bandwidth or equipment won't support it, you should consider a conferencing tool that provides VoIP functionality.

Converging Technologies

In the coming years, communication technologies—email, IM, voice, Web conferencing, collaboration tools—will begin to converge into a comprehensive unified communications (UC) platform. Gartner defines UC products (equipment, software, and services) as those that "enhance individual, workgroup, and organizational productivity by enabling and facilitating the control, management, integration, and use of multiple enterprise communication methods. UC products achieve this through the convergence and integration of communication channels, networks, systems, and business applications."

Under UC, audio and Web conferencing solutions will converge and include integrated presence information, letting users initiate an IM session, switch to audio or Web interaction, then invite other people into the conversation and seamlessly switch to a live conference. Microsoft is spearheading the push toward integrating conferencing functionality into the enterprise communications architecture. Live Meeting 2007 integrates multiple communication channels, including VoIP and Public Switched Telephone Network audio, chat, audience feedback tools, screen and document sharing, and live and recorded video.

Interwise is another leader in this area. Vice President of Marketing Neil Lieberman told me that the barriers between voice and Web communications are melting, and the trend is toward consolidation so that organizations have fewer products to buy and support. Interwise Connect combines voice, Web, and video conferencing into one product that uses a single data stream. Lieberman said the company's goal is to consolidate multiple communication and conferencing tools into one product and transform conferencing into a companywide core business application for all employees, like email is today.

Companies looking for a new conferencing solution should keep this trend in mind and plan accordingly. To map out a migration to UC, companies need to outline their current and future performance needs, scalability requirements, user expectations, integration with other business systems, and compatibility with legacy equipment.

Enterprises that want to wait until the UC technologies and markets mature might consider a short-term hosted service or pay-as-you-go solution. When the time comes to purchase a solution, they can use their experience to select one that meets their needs.

Organizations that are planning to update a companywide communications system certainly need to look at solutions that combine their voice and data networks. Thanks to the ease of integrating IP communications and traditional telecommunications systems, those companies will be able to to make the move in phases, minimizing user disruption and spreading the expense over time.

Ease of Use

Usability is key to a solution's success, making it one of the primary factors to consider when comparing Web-conferencing solutions. Does the service or product let you easily schedule meetings and invite guests using preferred desktop tools such as email and calendar applications? Does it have an intuitive UI that requires little training? Is it easy to deploy and manage? A tool that's difficult to use, manage, or maintain or that requires substantial training or IT involvement will dilute the solution's benefits and cost savings.

Citrix GoToMeeting is one of the easiest Web-conferencing tools to use and administer, and Sonexis's plug-and-play ConferenceManager is easy to set up and use. Other solutions known for their ease of use are WebEx Meeting Center and **SiteScape** Zon, both of which let you simply click a URL to download the conferencing client and begin a conference—no installation or maintenance is necessary.

Just the Basics

Basic features that every service or product should offer include broad Web-browser support, good security, and scalability. Additional features can mean additional complexity, so

THREE GREAT REVIEWS FOR

THE BOMGAR BOX™

"one of the best help-desk support solutions examined by the CRN Test Center"

CRN TEST CENTER RECOMMENDED ★★★★★ 5 STARS

June 21, 2007
Bomgar B300™
Version 9.3

"a direct link into problem Windows and Mac machines"

NETWORKWORLD CLEAR CHOICE 4.65 OUT OF 5

January 8, 2007
Bomgar B200™
Version 9.1

"a cost effective, secure, elegant hardware solution for remote customer support"

PC MAGAZINE www.pcmag.com ●●●●○ 4 Stars

May 7, 2007
Bomgar B100™
Version 9.2

TEST DRIVE BOMGAR TODAY 866.205.3648 | WWW.BOMGAR.COM/ITPRO

BOMGAR™

The Box That's Revolutionizing Remote Support™

you should select only the functionality you need, especially if the vendor charges more for certain features or services.

An online conferencing application needs to support common Web browsers, such as Microsoft Internet Explorer and **Mozilla** Firefox, and should provide integrated audio or support for third-party audio providers. Look for easy-to-use scheduling and invitation options, preferably through integration with common email and calendaring programs.

If you're considering a SaaS solution, make sure it provides the level of security you need. At the least, the service should offer Secure Sockets Layer or Transport Layer Security, 128-bit Advanced Encryption Standard encryption, and access controls such as secure logon, participant lists, one-time meeting IDs, and meeting passwords. If you buy a standalone solution, it will run within your organizational firewall, so you'll have total control of the application's security.

The solution you choose should also scale to fit your requirements. Does it need to support only meetings with fewer than 10 participants, or do you plan to hold large-scale presentations with hundreds of attendees?

Desirable Features

In addition to those basic features and considerations, some other components are widely considered to be must-haves. Probably the most basic and important of those is the ability to present slides, typically through PowerPoint.

Document-sharing functionality lets meeting participants collaborate in real time on documents, spreadsheets, and graphics. The most convenient method for sharing documents is to have one copy in a secure, private online meeting space and let meeting participants change and annotate that copy so you don't have to deal with multiple uploaded versions.

Desktop sharing lets the meeting host show anything on his or her computer to remote conference attendees. Most applications let presenters choose whether to share their entire screen or only a portion of it to keep the audience focused on key information. Desktop sharing is especially useful for interactive software demos.

Application sharing lets the host share any application on his or her computer desktop with participants. If this feature interests you, be aware that because it places a high demand on users' PCs, it might not be feasible for all users.

A whiteboard feature can be very valuable, especially when people meet to collaborate on a project. A whiteboard is a blank page that lets presenters draw diagrams and write notes on the screen—a useful capability for brainstorming sessions or for highlighting specific features of a presentation. Features that support participant annotation let attendees mark up the whiteboard presentation, often using a unique user-specific color.

Bells and Whistles

To get the most benefit from your conference solution, you might want even more features. Depending on how you expect to use the product, the following capabilities might be as essential as the basics, or they might simply be fluff that you'll rarely use:

- **Audience monitoring.** Most Web-conferencing applications have a window that lists attendees and their Web and audio status, and many let the host monitor who enters the conference and bounce unwanted attendees.
- **Co-browsing.** A co-browsing feature lets members of a Web conference simultaneously view the same Web page as the presenter or moderator. Co-browsing can distract users from the presentation, so make sure you can disable this feature if necessary.
- **IM and chat**. Chats allow real-time, private communication among attendees and presenters. Some applications provide private virtual meeting rooms in which two or more attendees can conduct a side-meeting via IM. IM and chats can also be distracting, so you'll want to be able to turn off this feature if necessary.
- **Polls**. Polls let presenters survey audience members for real-time feedback. Some solutions can present the results to attendees as graphs and charts.
- **Ad hoc meetings.** Many applications require you to set up and schedule the conference and invite attendees in advance, but one trend is to allow ad hoc meetings from within applications such as email, IM, or your phone system. This capability lets you begin a meeting spontaneously and, if integrated with presence information, invite the appropriate attendees.
- **Ongoing meetings.** With ongoing-meeting functionality, virtual meeting rooms can retain all meeting documents, annotations, edits, whiteboard content, and text brainstorming sessions, letting you reconvene an interrupted meeting and providing a convenient way to store and reuse conference materials.
- **Record and replay.** The ability to record and archive Web conferences lets people who couldn't attend the meeting access the session later to see what they missed, making it easier and quicker for interested parties to bring themselves up-to-date. Recorded meetings are also useful for future reference.
- **Branding.** A branding feature lets companies customize the logon page and other areas with logos, pictures, colors, and fonts.
- **Video.** Some applications let participants who have WebCams see each other.

That high-level overview of the types of features and functionality in today's Web-conferencing tools should give you an idea of which ones are important to your organization. Different solutions provide various combinations of these features, either built in or for an added charge, and implement them with varying degrees of usability and robustness. Most solutions offer a free trial version or a free demo so you can try before you buy.

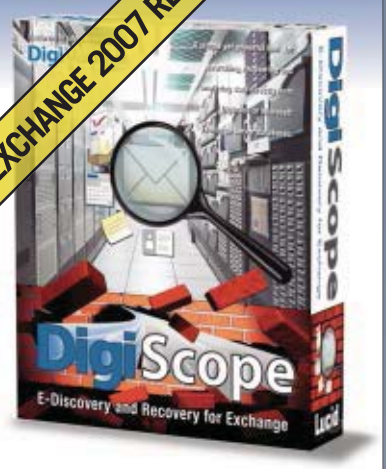
Sparking Ideas

The pricing or licensing model and how well the application integrates with existing hardware and software might be more important to you than the specific feature set, but understanding the range of functionality available can spark ideas for leveraging a conferencing solution for maximum benefit and productivity. Although use scenarios are beyond the scope of this article, activities such as employee training, sales presentations, line-of-business collaboration, project development, and brainstorming are among the most common. Organizations that rely solely on traditional linear methods of communication—such as face-to-face, phone, fax, voicemail, and email for such activities—fail to take advantage of the rich media opportunities that Web conferencing can provide. As the technology continues to evolve, it will become an indispensable tool for enhancing collaboration and productivity and minimizing communication costs.

InstantDoc ID 96579

Gayle Rodcay
(gayle@windowsitpro.com) is a senior editor for *Windows IT Pro* and *SQL Server Magazine*.

EXCHANGE 2007 READY!



Created By

Lucid

Solutions Inspiring Confidence

- FIND MESSAGES, ITEMS, & CONVERSATION THREADS
- EXPORT TO PST, MSG, OR XML IN RAW, ZIP, OR ZIP ENCRYPTED
- RECOVER OR COPY ENTIRE MAILBOX, FOLDER STRUCTURE OR SELECTED ITEMS
- PROTECTS EVIDENCE CHAIN

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

Microsoft GOLD CERTIFIED Partner

FREE DOWNLOADS

- Demo version of DigiScope
- White Paper –"The Federal Rules of Civil Procedure, E-mail Discovery and You." by Osterman Research

Go to: www.Lucid8.com/Discover
Call: 425 456-8493
E-Mail: Sales@Lucid8.com

Top 8 Tips for Email Discovery and Recovery

Obviously, backing up your Exchange server is quite critical, however, backup is only a small part of the solution. Anyone can click through the three or four steps required to run a backup to tape or disk, but what happens if you have to recover a user's entire mailbox or perhaps just a handful of emails that someone accidentally deleted?

If you received a court order to produce an e-mail thread from three years ago, could you do it? How about within three working days? New guidelines such as the Federal Rules of Civil Procedure (FRCP) require an exhaustive search for all electronically stored information, including all email that is "in the possession, custody, or control of the party."

Those of you that have or will be implementing an archiving solution such as Symantec Enterprise Vault or EAS from Zantaz, may be a bit more prepared, however, unless you ingested every email sent and received within your organization from every tape and PST file that exists into the email archive (and nobody has) you are still at risk (See Tip 2 below).

Tip 1: A single solution for restores and discovery

Restoration and Discovery requests are essentially the same thing; each is a call to look through your Exchange databases or backups and find specific items. Restores go further by putting the item back from where it came and discovery takes a different route by exporting the recovered items somewhere else, typically a PST file. It therefore makes sense to choose a single product that can do those two things rather than stick to the conventional wisdom that restore and discovery jobs call for separate tools.

Tip 2: Simplified discovery

If you are required to implement and maintain an archive of your old email information, your archiving product will only work from the point in time that you commission it. What about that critical email that was deleted two days before the mailboxes became subject to archiving? The information may be on an old tape, disk backup, or PST file but it's not in the current Exchange Information Store or in the email archive system. It is Murphy's Law that the one item that will prove the innocence of your corporation in whatever it is defending will be located in one of tens, hundreds, or thousands of "orphan" backup tapes or PST files. Clearly you need a product for searching, recovering, and exporting the required information from previous backups and PST files that haven't made it into the email archive.

Tip 3: Multiple sources

The problem with most item-level restoration products is that they can only look at one source at a time. This is always annoying because you often don't know where in your backups the item you're looking for is. If, in a discovery operation, you happen to know where the original item is do you know where all the replies and related materials are? Select a discovery application that can simultaneously open multiple information stores, as well as PST's, and search across all data sources in a single operation.

continued on back

Tip 4: Public folders, Granular item-level, and Legacy mailbox recovery with the Recovery Storage Group (RSG)

In many cases, organizations will be asked to provide all email or items from individual mailboxes as well as public folders within a date range for all existing as well as legacy users. The problem is Microsoft simply doesn't support public folders or granular item-level recovery from existing mailboxes using the RSG. Furthermore, even if you have a backup of a store that contains the legacy user's mailbox, once a legacy user's mailbox has been deleted from Exchange and Active Directory the information cannot be accessed or recovered using the RSG. You need a solution that offers the ability to access, search, restore, or export all historical information, even if the legacy user no longer has a mailbox or AD account.

Tip 5: Formatting

Whatever solution you choose to use for discovery and restoration it must also be able to export the data in a format that can be used by the organization requesting the recovery. There is little point in extracting messages into a PST file if the requester cannot accept such a file, or it's in a proprietary format not widely used. Far better is to ensure that your solution can, if necessary, export data into formats such as the standard '.msg' format or XML format. Of course, the PST format is widely used so make sure your solution can still use that format as well as the others.

Tip 6: Optimize your backups

The traditional way of performing backups that enables the restoration of a single item is to do the backup twice. One backup takes the entire store in one pass. Then individual mailboxes are backed up again—sometimes referred to as brick-level backup—with a slow, tape-consuming second run where each mailbox is backed up into a physical entity from the logical entity that exists in an information store. The tip here is to do your backup once with something as basic as you can; the included application, ntbackup.exe, is more than good enough to complete this once a day task. Keep in mind, however, that a full or incremental backup performed at midnight leaves a full 24 hours of corporate productivity completely vulnerable. You can of course close the 24 hour gap by implementing a Continuous Data Protection (CDP) product that will provide up-to-the-minute protection of all Exchange data. Either way once you have the backup on tape or, better yet, inexpensive disk resources, you can use an advanced recovery and discovery tool to access the information you need.

Tip 7: Legacy information

These days nearly everyone exports a departed or terminated user's mailbox to a PST file to free up space in the stores, or simply to maintain a safe copy, thus rendering it inaccessible to other discovery methods. Again, with more and more regulations affecting more and more companies you cannot afford to have all these PST files stored on various media in ever-changing locations. Keep all the information inside the store and make sure there is a full backup of that store. Once you're happy that the store is secured and you can recover it, or items from it, you can delete the mailbox and account. While you might always know where the Exchange backups are, do you always know where all your PST files are located? Do you always take the same amount of care of the media on which the PST files are stored as you do with the normal Exchange backup media? Ensure that your Recovery/Discovery tool has the ability to search across multiple information stores as well as PST files.

Tip 8: It's not your job

Your Human Resources department will be the one to most often make discovery requests so why should it not be the one that does the searches. Well, all too many products have interfaces that require a degree in rocket science to use, which dissuades the HR department from taking on the duty that is theirs by right. Choose an application that has a simple-to-use interface, preferably one that even looks and acts the same as your corporate standard email client. IT departments always have resource constraints; make sure you don't make matters worse for yourself by choosing an application that only you can use.

Choosing the backup application to use is relatively straight forward, the simpler the better. The restore application can be the same application that you used to back up or it can be as advanced as you need. Wrapping up your restoration process with a discovery application reduces the complexity of the environment while at the same time allowing you to retain more information with less infrastructure.

Avoid Disaster with UPS

Begin your search for the perfect power-backup hardware

As I write this article, hurricane season is underway, and according to the local research team here at Colorado State University (reported by National Geographic and ScienceDaily), 2007 could be a very active hurricane season, including possible storms with winds over 111 miles per hour. Hurricanes aren't much of a threat in Colorado, but I can't help but think about the kinds of disasters that can strike an organization. Since Hurricane Katrina, everyone seems to be a little more focused on taking preemptive measures to protect against all sorts of disasters.

On top of natural disasters, you also have to worry about power outages and sudden spikes in power, which can severely affect your day-to-day business operations. A disaster-recovery plan has many facets—offsite backups, recovery plans, and so on—and one of the most essential aspects of that plan should be a UPS. This hardware can continue computer and server operations even if your system power fails, letting you save data or close critical applications.

The Backbone of UPSs

The UPS market is a fairly mature market and hasn't changed much over the past year or so. There are still three main types of UPSs. The cheapest type—aimed primarily at desktop computers—is the standby UPS. This type uses the commercial AC line as its primary power source, and when a power outage or voltage drop occurs, the primary source switches from the AC line to the UPS's internal battery. However, the switch between power sources isn't instant. Remember, the quicker the UPS takes over your equipment's power, the quicker you can save critical data and close important applications. The second type, line-interactive, uses an inverter/converter that serves two purposes: charge the UPS's internal battery and convert the battery's DC power to AC power to run your connected equipment. The advantage of this type is that the inverter/converter is always connected to the UPS's output, providing a faster response time to power failure. The third type—and the greatest protection for your systems—is the online UPS. An online UPS doesn't rely on the AC line but rather uses a battery as its primary source, never having to transfer power between different sources.

One consistent factor among UPSs is output capacity, measured in VAs. As you narrow in on the right UPS, talk with the vendor to ensure that the UPS you're considering can power your current equipment and any future equipment you plan to purchase. For this buyer's guide, I've focused on floor-mounted UPSs for small-to-midsized businesses (SMBs) that protect 10 servers or fewer, and with a limit of 6,000VA.

Windows UPS Service

If you've already installed a UPS—or you plan to do so in the future—you can use the Windows UPS Service to manage its operations from your server. The Windows UPS Service isn't new, by any means. You can find it in Windows XP, in the Control Panel Power Options applet. For instructions about using the Windows UPS Service to configure, install, use, remove, and test a UPS device, see the Microsoft article "Using the Uninterruptible Power Supply (UPS) service" (http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/pwrmn_ups_overview.mspx?mfr=true).

Management Platform

Most vendors will have some sort of management platform to manage the UPS infrastructure. Having one central location to monitor all power usage can be a lifesaver, particularly if you have several UPSs. And application-shutdown support can also be extremely useful—saving you from having to do the work manually during a disaster situation. When power outages occur, IT has to scramble to do many things. This functionality takes one task off the plate.

Staying Green

It's no secret that large companies are spending lots of money on powering day-to-day operations. This increase in powering costs has produced a number of studies and vendor initiatives on "green technology." The challenge is to find ways to reduce the amount of power we produce—with the nice byproduct of reducing costs.

Green-technology efforts have mostly focused on large data centers, but even if you're managing a branch office or running your own small business, you can save energy and money. Watch for power-saving features in the UPS you're considering. Such functionality primarily provides automatic, unattended shutdown. Other power-saving features include the ability to shed less critical loads (turning off individual UPS outlets) and log of power-consumption patterns.

Start Your Research Here

One of the best ways to prepare your business for any kind of disaster is to invest in UPS hardware. There are many factors to consider, so you're in for a little research. On the following pages, you can begin your shopping.

InstantDoc ID 96810

Blake Eno
is former product editor for *Windows IT Pro* and *SQL Server Magazine*.

EDITOR'S NOTE

The Buyer's Guide presents vendor-submitted information. To find out about future Buyer's Guide topics or to learn how to include your product in an upcoming Buyer's Guide, go to http://www.windowsitpro.com/buyersguide.

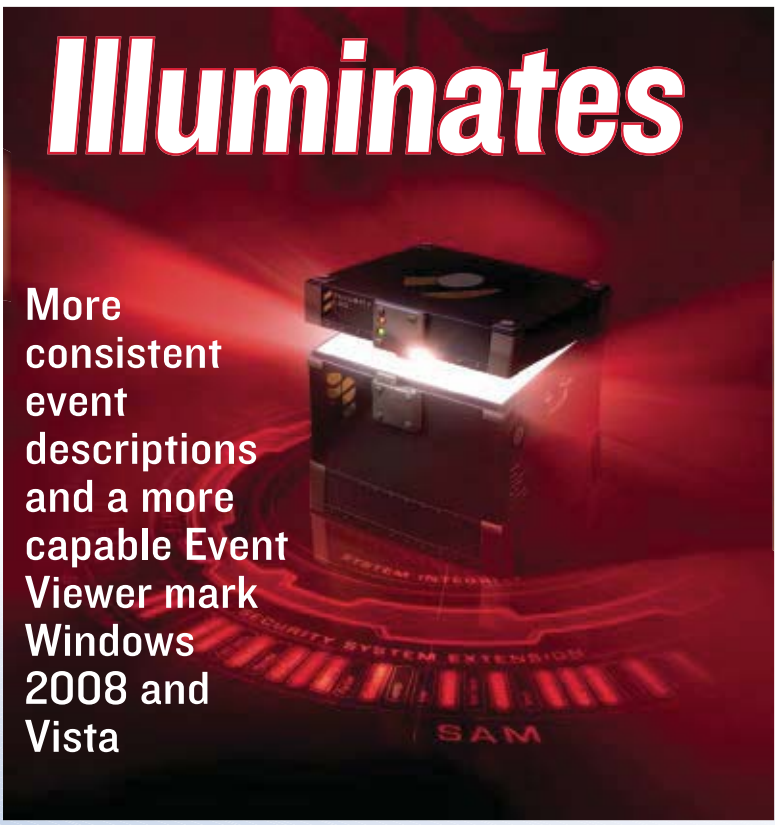
Contact Information	Product	Price	Number of Servers the Unit Protects	Output Capacity	Type	Dimensions
American Power Conversion http://www.apcc.com 877-272-2722	Smart-UPS Series	$310-$1,150	Depends on power	750VA-3,000VA	Line-interactive	5.4"-17" x 14.1"-21.5" x 3.5"-17"
	Smart-UPS SC Series	$330-$409	Depends on power	1,000VA-1,500VA	Line-interactive	17" x 18.24" x 3.5"
	Back-UPS RS Series	$220-$250	Depends on power	1,300VA-1,500VA	Line-interactive	8.75" x 5.25" x 14"
	Smart-UPS XL Series	$449-$1,350	Depends on power	1,000VA-3,000VA	Line-interactive	6.7"-7.7" x 17.3"-19" x 8.5"-17"
Belkin http://www.belkin.com 800-223-5546	F6C1500-TW-RK	$200	8	1,500VA	Line-interactive	3.5" x 13.25" x 15"
Clary http://www.clary.com 626-359-4486	Clary DT Series	$3,750	3-5	2,000VA	Online	17" x 20.25" x 9.3"
	Clary E603 Series	$8,900	10 or more	6,000VA	Online	12.3" x 28.7" x 26.8"
Falcon Electric http://www.falconups.com 800-842-6940	SG Series	$746-$4,789	1-9	800VA-6,000VA	Online, Double Conversion	6"-10.2" x 15.8"-30" x 8.7"-32.1"
	SSG Series	$1,390-$2,989	2-4	1,500VA-3,000VA	Online, Double Conversion	16.8" x 21.5" x 3.5"
	FN Series	$3,889-$4,998	4-9	3,000VA-6,000VA	Online, Double Conversion	11.5" x 25.4" x 29.5"
MGE Office Protection Systems http://www.mgeops.com 800-523-0142	Pulsar Evolution Series	$355-$1,391	1-6	500VA-3,000VA	Line-interactive	5.9"-17.2" x 13.9"-25.2" x 1.73"-9.3"
	Pulsar EX RT Series	$635-$1,871	1-6	700VA-3,200VA	Online	17.25"-19" x 3.46"-25.75" x 3.4"-25.75"
	EX RT 1:1 Series	$3,903-$7,935	1-10 or 1-2 blade servers	5,000VA-7,000VA	Online	17.49" x 25"-28" x 10.32"-15.48"
	Pulsar MX Series	$3,936-$5,182	1-10 or 1 blade server	5,000VA	Online	17.5" x 27.6" x 5.14"-8.75"
Toshiba http://www.toshiba.com 800-231-1412	1000 Series	$849-$2,166.65	1-12	1,000VA-2,000VA	Online	16.5"-16.7" x 6"-16.9" x 3.5"14.2"
	1600EP Series	$5999-$7399	Depends on load	3,600VA-6,000VA	Online	33" x 10" x 28"
Tripp Lite http://www.tripplite.com 773-869-1111	SmartPro UPS System Series	$299-$1,029	4-10	750VA-3,000VA	Line-Interactive	10.25"-17" x 6.75" - 9.25" x 7.25" - 16.75"
	SmartOnline UPS Systems Series	$449-$1,299	6-9	750VA-3,000VA	Online	10"-10.25" x 6.75"-9" x 13.25"-20.5"

EDITOR'S NOTE: Some vendors that you might expect to see in this Buyer's Guide said they didn't have a product that exactly matched the criteria or didn't

	Battery Recharge Time	Outlets	Backup Time at Full-Load	Communications Port	External Battery Pack Support	Remote Management	Power-Saving Features	Warranty	On-Site Service
	3-6 hrs	4-10	4.6 mins-8.8 mins	USB, Serial, EPO and Smart-slot for optional RJ45	No	Yes	No	2-year warranty	Yes
	8 hrs	6	7.4 mins-7.6 mins	Serial + USB (with supplied adapter cable)	No	Yes	No	2-year warranty	Yes
	16 hrs	8 outlet, 6 UPS, and 2 surge	5 mins	LCD plus USB and Serial Tel/Coax and Net Protection	No	No	No	3-year warranty	Yes
	3-6 hrs	8-11	5.5 mins-16.6 mins	USB, Serial, EPO and Smart-slot for optional RJ47	Yes	Yes	No	2-5 year warranty	Yes
	< 12 hrs recover 85% capacity	8	4 mins	Ethernet	No	Yes	Yes	3-year warranty	No
	8 hrs to full charge	4	5 mins	RS232, Ethernet, and dry contacts	Yes	Yes	Yes	2-year warranty	Return to factory
	1.5-3 hrs	Hardwired	8 mins	RS232, Ethernet, and dry contacts	Yes	Yes	Yes	2-year warranty	GE Service Group
	8-10 hrs	1-6, hard-wired	5.5 mins-11 mins	Yes	Yes	Yes	Yes	2-year warranty	Yes
	8 hrs	5-8	5 mins-8 mins	Yes	Yes	Yes	Yes	2-year warranty	Yes
	4 hrs	Hardwired; external PDU available	12 mins-31 mins	Yes	Yes	Yes	Yes	2-year warranty	Yes
	3-4 hrs to 90% capability	6-8	4.5 mins-7 mins	USB & Serial, Optional Ethernet	Yes/No	Yes	Yes	2-year warranty	N/A
	3 hrs to 90% capability	4-10	6 mins-12 mins	USB & Serial, Optional Ethernet	Yes	Yes	Yes	2-year warranty	N/A
	5 hrs to 90% capability	Hardwired plus 10 outlets	7 mins-9 mins	Serial, Optional Ethernet	Yes	Yes	Yes	2-year warranty	Installation & Start-Up
	6 hrs to 90% capability	4-11 plus Terminal block for hardwired output	5 mins	USB & Serial, Optional Ethernet	Yes	Yes	Yes	2-year warranty	Installation & Start-Up
	3.5 hrs	4-12	6 mins-7 mins	USB, Serial, Dry Contact, Ethernet (Network)	Yes	Yes	No	3-year warranty	Yes
	12 hrs	Different options available	7 mins	Serial, Dry Contact, Ethernet (Network)	Yes	Yes	No	3-year warranty	Yes
	2-8 hrs to 90%	4-10	3.5 mins-12 mins	DB9, USB, Ethernet, EPO	Yes/No	Yes/No	Yes	2-year warranty	Yes
	4-6 hrs to 90%	6-10	4 mins-5 mins	DB9, USB, Ethernet, EPO	Yes	Yes	Yes	2-year warranty	Yes

respond to our requests for information about their products.

NEW SECURITY LOG Illuminates



BY RANDY FRANKLIN SMITH

Windows Server auditing and the Security event log have really changed in Windows Server 2008 and Windows Vista, and I'm glad to say that most of the changes are good. The Security log is a little cleaner and a little easier to understand, but you still need a lot of knowledge about Windows security and experience in decoding mysteries to really "grok" it. I've spent the last decade deep in the bowels of Windows security and auditing, and lately I've been concentrating on Windows 2008 and Vista, so maybe I can help bring you up to date with the changed event ID numbering, the new, more granular way that audit policy is handled in Windows 2008 and Vista, the XML log format, and enhancements to the Microsoft Management Console (MMC) Event Viewer snap-in.

New Event IDs

If you're already familiar with the Windows Security log, the first thing you'll notice when you open Event Viewer in Windows 2008 is that none of the old event IDs shows up. That's right! Just when you thought you knew the difference between event ID 528 and event ID 529, Microsoft goes and changes the IDs. Actually, Microsoft kept many of the events found in Windows Server 2003 but added 4,096 to the event ID. For instance, event ID 528 in Windows 2003 is event ID 4624 in Windows 2008.

I'm actually glad Microsoft changed all the event IDs because the company also completely revamped the fields in the description of each event. In Windows 2003, Microsoft kept event IDs from Windows 2000 Server but changed the events that they track, combined multiple event IDs into one, and changed the order of fields in the descriptions. This wreaked havoc on automated log analysis software. The new numbering lets you add Windows 2008 systems to your environment and begin collecting logs without throwing off your existing filter, alert, and reporting definitions. You *will* have to add new definitions for the new event IDs.

Audit Policy Subcategories

One of the most frequent questions I've gotten from people over the years about the Security log is how to stop Windows from logging so much #%*@&! noise (i.e., useless events that make finding the important events that much more difficult). My response has always been, "You can't configure the noise out of the Windows Security log; that's the job of your log management solution."

ILLUSTRATION BY RYANETTERILLUSTRATION.COM

Windows Events

Well, Microsoft has taken a small step in the direction of helping you quiet things down. The company didn't do it the way I would have, which would have been to introduce a firewall-like rule set that would let you define on an event-ID-by-event-ID basis criteria for whether to record the event. Instead, Microsoft expanded the 9 audit policies (aka categories) in Windows 2003 to 52 in Windows 2008.

Actually, Microsoft kept the existing 9 policies and broke them into subcategories, each of which you can enable for success and/or failure events. If you like, you can still manage audit policy with the 9 top-level categories. Figure 1 shows the 9 categories and 52 subcategories. (See http://www.ultimatewindowssecurity.com/newauditpol for a table that decomposes the 9 categories into their respective subcategories and provides a brief description of what kind of events and activity each category tracks.)

This is all good news so far. In fact, you can eliminate a number of old noisy events with this more granular audit policy as well as disable some of the new event IDs logged by Windows 2008, which are pretty noisy as well. For instance, most of you will want to disable the Filtering Platform Packet Drop and Filtering Platform Connection subcategories, which are extremely noisy because they record network traffic at the packet level.

But here's some bad news: You can't manage audit policy at the subcategory level by using Group Policy. Microsoft added the 52 new subcategories but didn't update Group Policy with new policies to enable or disable the subcategories. In fact, you won't find these subcategories anywhere in the GUI. The only way to enable or disable at the subcategory level is with the Auditpol command. The Microsoft article "Security auditing settings are not applied to Windows Vista client computers when you deploy a domain-based policy" (http://support.microsoft.com/kb/921468) proposes a method for configuring audit subcategories via startup scripts defined via Group Policy, but the technique is something Rube Goldberg would be proud of.

Working with Audit Policy

Let's delve a little into the Auditpol command as well as how Windows resolves possible conflicts between the audit policy you configure in Group Policy Objects (GPOs) and the subcategory policy you can configure with Auditpol. To find out the current status of your 52 audit subcategories, just log on to the desired system and type

```
auditpol /get /category:*
```

at the command prompt. This command produces output similar to that shown in Figure 1. As you can see, the 9 top-level categories are listed with their subcategories below and whether each is enabled for success and/or failure.

To change auditing for a subcategory, just run auditpol with the /set command and specify the subcategory and whether to enable success and/or failure events. For instance,

```
auditpol /set
  /subcategory:"System Integrity"
  /failure:enable /success:enable
```

enables the System Integrity subcategory for both success and failure events.

But what if you configure audit policies for the 9 top-level audit categories in Group Policy that conflict with policies set for the 52 subcategories in Auditpol or vice versa? For instance, let's say your computer W08-YHWH resides in the Servers organizational unit (OU) in Active Directory (AD). You edit a GPO linked to that OU to disable the *Audit logon events* (aka Logon/Logoff) top-level category for both success and failure. Then you log on to W08-YHWH and, with Auditpol, you enable the Logon subcategory for success and failure. What will the final outcome be?

By default, if you define a value for one of the 9 top-level categories either in the computer's Local Security Policy or in an applicable GPO, the top-level policy will override the configuration at the subcategory

Category/Subcategory	Setting
System	
Security System Extension	Success and Failure
System Integrity	Success and Failure
IPsec Driver	Success and Failure
Other System Events	Success and Failure
Security State Change	Success and Failure
Logon/Logoff	
Logon	Success and Failure
Logoff	Success and Failure
Account Lockout	Success and Failure
IPsec Main Mode	Success and Failure
IPsec Quick Mode	Success and Failure
IPsec Extended Mode	Success and Failure
Special Logon	No Auditing
Other Logon/Logoff Events	Success and Failure
Network Policy Server	Success and Failure
Object Access	
File System	Success and Failure
Registry	Success and Failure
Kernel Object	Success and Failure
SAM	Failure
Certification Services	Success and Failure
Application Generated	Success and Failure
Handle Manipulation	Success and Failure
File Share	Success and Failure
Filtering Platform Packet Drop	No Auditing
Filtering Platform Connection	No Auditing
Other Object Access Events	Failure
Privilege Use	
Sensitive Privilege Use	Failure
Non Sensitive Privilege Use	Failure
Other Privilege Use Events	Failure
Detailed Tracking	
Process Termination	Success and Failure
DPAPI Activity	Success and Failure
RPC Events	Success and Failure
Process Creation	Success and Failure
Policy Change	
Audit Policy Change	Success and Failure
Authentication Policy Change	Success and Failure
Authorization Policy Change	Success and Failure
MPSSVC Rule-Level Policy Change	Success and Failure
Filtering Platform Policy Change	Success and Failure
Other Policy Change Events	Success and Failure
Account Management	
User Account Management	Success and Failure
Computer Account Management	Success and Failure
Security Group Management	Success and Failure
Distribution Group Management	Success and Failure
Application Group Management	Success and Failure
Other Account Management Events	Success and Failure
DS Access	
Directory Service Changes	Success and Failure
Directory Service Replication	Success and Failure
Detailed Directory Service Replication	Success and Failure
Directory Service Access	Success and Failure
Account Logon	
Kerberos Service Ticket Operations	Success and Failure
Other Account Logon Events	Success and Failure
Kerberos Authentication Service	Success and Failure
Credential Validation	Success and Failure

Figure 1: Sample Auditpol output

level. Under Windows default behavior, your subcategory policies take effect only if you leave the top-level category undefined in the Local Security Policy and in all applicable GPOs. I stress *default behavior* because a new setting in the Group Policy Object Editor (GPE) under Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options called *Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings,* if enabled, reverses audit policy behavior so that whatever you configure for the subcategories in Auditpol overrides how the 9 top-level policies are set by the applied Group Policy.

I can't believe that Microsoft let Vista, much less Windows 2008, out the door without making this extremely important and sensitive area of security configuration manageable via Group Policy, but it did. And the solution set forth in the above Microsoft article is flimsy and prone to failure, in my opinion. The other amazing thing is that you can't run Auditpol against remote computers—only against the local system.

Anyway, here's what I recommend as a starting point for your audit policy in terms of top-level categories: Enable System, Policy Change, Logon/Logoff, Account Logon, Account Management and, on domain controllers (DCs), DS Access, which gives you the ability to track important changes to OUs and GPOs. Enabling these categories for success and failure will get you your most important information while eliminating major sources of noise such as Privilege Use and Object Access. If you do need to perform some file system auditing, then enable Object Access's File System subcategory.

After you enable the top-level categories you want by using GPE, use Auditpol to turn on success and failure auditing for each desired subcategory as shown above.

Selectively disable subcategories to eliminate events you don't want. To discover and confirm which subcategories to disable, identify events you don't want in Event Viewer and determine their subcategory name, which is known as the Task Category in Event Viewer. Before disabling a subcategory, make sure you don't need any other events belonging to that subcategory and success/failure type. To make that decision, filter the log in Event Viewer to show only the events in that subcategory.

IT Pro Hero

Anatomy of a Botnet

BY B. K. WINSTEAD

With the help of a sniffer and some IT detective work, David Soussan found a botnet at the root of a client's network problem

David Soussan got hooked on computers when he took a FORTRAN programming class in junior high. Now the owner of DAS Computer Consultants, David recently encountered a perplexing network troubleshooting challenge at a client site. The company's Internet access was down, and David's initial investigation pointed to a bad firewall. However, the problem was actually something much worse: a botnet that was commandeering the company's systems. David and I discussed how he uncovered the worm's trail and what IT pros can learn from his experience.

Q: Explain the client's network problem and how you investigated it.

A: The client's ISP said, "It looks like [the network is] up, but we're seeing some funny traffic." From inside the LAN, I got echoes pinging the firewall but not the WAN router. Then I tested the Internet connection by disconnecting the WAN router and firewall and attaching a single client to the WAN. The ISP was right: The Internet connection worked, so I knew the problem was related to the LAN. I reconnected the firewall to the WAN router, connected the PC to the closest switch, and still couldn't ping the WAN. It appeared to be a firewall problem. I replaced the firewall with another product, and the LAN worked OK. But when I tested the firewall offline, it was good.

I suspected that traffic on the LAN was killing the firewall, so my next step was to use a network sniffer to view the traffic going into the firewall. The initial sniff looked like a lot of junk flying around the LAN. By applying a succession of smaller and narrower filters, I found that one particular system's traffic was suspicious because the system was attempting connections to many machines.

I disconnected that machine—a Windows 2000 server—from the LAN. The next step was to determine what on that computer was sending out the bad traffic. I rebooted the suspect system, then ran Mark Russinovich's TCPView and Process Explorer tools on it to see what programs might be opening network connections and what their traffic was doing. I started the sniffer, then connected it to the LAN long enough for it to get an IP address. TCPView lit up like a Christmas tree, showing a couple of hundred connections that instantly formed to batches of addresses all over the Internet. The program making all these connections was called ifconfig.exe in c:\windows\system32.

You can also refer to my free Windows Server 2008 Security Log Encyclopedia at http://www.ultimatewindowssecurity.com/encyclopedia.apx for a listing of events by category. If you determine that no important events are logged by that subcategory for the same success/failure type, use Auditpol to disable the subcategory for success, failure, or both (as appropriate).

Don't forget that if you want your subcategory settings to take effect, you'll need to change the Group Policy setting *Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings,* as mentioned above.

Event Format

Now, let's discuss the new format that events have in Windows 2008. Microsoft changed both the physical file format of the Windows event logs as well as the logical fields that comprise each event sent to the log. If you're an XML buff, the XML schema for event logs is http://schemas.microsoft.com/win/2004/08/events/event; otherwise the new format doesn't impact administrators that much. If you're a developer dealing with event logs, Windows still supports the old Win32 Event APIs, but you might want to check out the new capabilities at http://msdn2.microsoft.com/en-us/library/aa382610.aspx. The Security Pro VIP article "Windows Eventing 6.0," September 6, 2007, InstantDoc ID 96587, also has a few more details about the new XML log and event formats.

The logical format of events (as displayed by Event Viewer in an event's properties dialog box) is much more important. Figure 2, page 40, shows event ID 4625. Each event still has a number of what I call standard fields as well as a text description. Standard fields provide information that applies to every event regardless of event ID—information such as the date and time of the event, the source, the category, and whether the event was a success or failure event. The message and data items in the text description vary from one event ID to another.

Each event ID's description is a combination of static text and dynamic insertion strings. In the text below, you see the first few lines of event ID 4625's description. The text in black is static; the values in red are specific to the particular instance of the event.

An account was successfully logged on.

Q: How did you determine that a botnet was running on the server?

A: When I viewed the ifconfig.exe process with Process Explorer and suspended it, ifconfig.exe claimed it was from Microsoft, but Process Explorer wouldn't verify ifconfig's digital signature. When I looked up the file in the c:\windows\system32 directory, it was marked read-only, system, and hidden. I opened ifconfig.exe by using the Attrib command, copied the file to a USB drive, and sneaker-netted the file to my notebook. When I copied the file from the USB key into my notebook, Trend Micro's antivirus software instantly flagged it as WORM_RBOT.CWU.

Next, I put the worm into an "isolation chamber" built with a Windows 2000 Server virtual machine (VM) running on my notebook. With Ethereal sniffing the network and the worm copied into the VM, I watched as the worm was started. It immediately disappeared from the desktop, copied itself into c:\windows\system32, and started making DNS queries to a dynamic DNS service in Hungary. Later I ran a Traceroute, which localized the target IP address to a dial-up account in Russia. The next morning, the bot client in the isolation chamber connected to its master, received orders, and started trying to exploit vulnerabilities in Symantec's antivirus product on port 2967 at various Internet locations.

Q: How did you get rid of the bot?

A: Network traffic from the sniff indicated that the bot was "phoning home" on TCP port 4212. From another sniff, I found that many client machines were also compromised and running the same worm. Meanwhile, the isolation-chambered worm was still checking every few seconds for its master, with no answer. My client runs its own DNS servers, which forward requests for out-of-their-domain names to the ISP's DNS servers. To prevent the worm from phoning home, I added a DNS record in their DNS servers telling the servers they were the authoritative DNS for the botnet's domain name.

I stopped the worm on one server and watched. It didn't respawn—evidence that it didn't have another program watching its back. I also carefully watched the network traffic to detect whether any other attempts were made to connect to anywhere else—and saw none. Deleting the ifconfig.exe file and removing run keys appear to be a valid fix, though I was cautious. We were lucky; this wasn't a very smart worm. We opted to leave the less-critical server's worms suspended and manually cleaned the critical servers.

I also blocked all access to port 4212 on the firewall. I knew that copies of the worm were still running on client machines. When I viewed the traffic on port 4212, I compiled a list of infected machines by IP address; the client's IT staff could deal with those.

Q: What can IT people learn from your experience?

A: The network was infected because the company was running an unpatched version of Symantec's antivirus software. There was a patch for the vulnerability that infected this computer, but this company's IT staff didn't apply that patch and roll it out. Also, the bot came in via a notebook that was used offsite, probably connected to someone's home DSL and unprotected by a firewall, and brought back into the corporation. So the lessons are, convince users who take data off site to be more careful and vigilant, and make patch management a priority. An unpatched system is a wide-open door to your corporate assets.

InstantDoc ID 96879

B. K. Winstead

(bwinstead@windowsitpro.com) is an assistant editor for *Windows IT Pro* and *SQL Server Magazine*, specializing in messaging and unified communications.

Read an expanded version of this article online at http://www.windowsitpro.com, InstantDoc ID 96879.

Subject:
Security ID: SYSTEM
Account Name: WIN-K2SF4WMIKI7$
Account Domain: ACME
Logon ID: 0x3e7

So that much hasn't changed—that is, the concept of standard fields and a description that's event ID specific. What has changed are the individual standard fields and the insertion strings logged by each event ID.

Compare event ID 4625 (Figure 2) to its predecessor, event ID 529 in Windows 2003 (Figure 3). Most of the changes to the standard fields are easy to figure out, such as Date and Time changing to Logged, but let me call out a few that might require a little explanation. First, notice that the old top-level category doesn't show up in Windows 2008 events because in Windows 2008, the top-level audit categories relate only to audit policy (i.e., which event IDs get logged and which don't). When Windows 2008 logs events, it resolves them down to their subcategory level, which Event Viewer calls the Task Category. Evidently being consistent with Auditpol and using *Subcategory* was too boring.

There's no longer any Type. Now, we have Level and Keywords. As far as I can tell, all events in the Security log appear to have the *Information* level, and either the *Audit Failure* or *Audit Success* keywords.

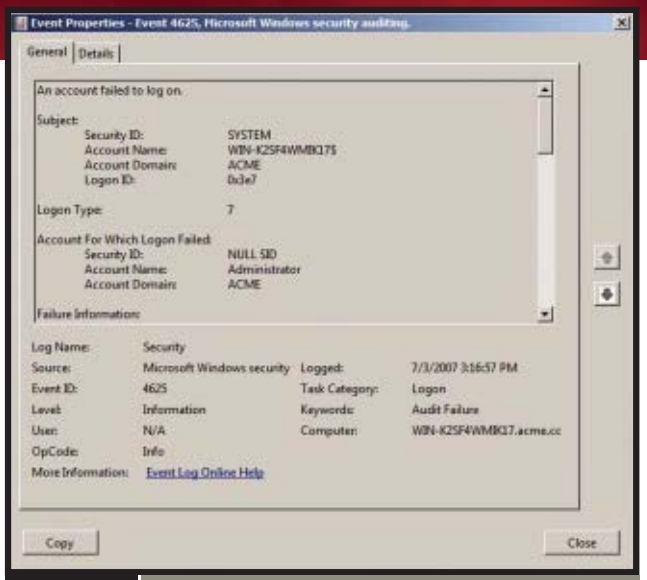


Figure 2: A sample event ID 4625

You'll find that the event descriptions have changed drastically. Windows 2008 inserts many more dynamic values in the descriptions, and Microsoft has made progress in enforcing some consistency in description data throughout the different event IDs. The event ID descriptions are a good example of how a well-designed XML schema helps handle data records that are similar in structure but dynamic from one instance to another.

Many event ID descriptions share common data elements. For instance, nearly every event needs to log subject information—that is, the "who" of the event. As Figure 2 and the text above show, subject information includes SID, account name, domain, and logon ID. Historically, Windows has been inconsistent from one event to another about exactly how it logged this subject information. Some subject data was sometimes omitted or labeled differently.

To see an example, compare the subject data in Windows 2003's Account Logon events. The account name is labeled several different ways, and certain subject data is missing from some event IDs.

In Windows 2008, you'll find a number of common sections across most event IDs. I already mentioned the Subject section. Events that track an operation on some type of object—such as access to a file—have an Object section with all the appropriate fields for identifying the object, such as the type of object and its fully qualified name. All events that note the system process involved in the event include a Process Information section that documents the process identifier (PID)

and name of the executable.

Finally, you'll find more explanatory text at the bottom of some event descriptions giving background on the event or explaining a little bit about some of the values in the description. But the coverage is pretty spotty and frequently incomplete. Whew! My Security Log Encyclopedia lives on!

New Event Viewer

I'll finish up by describing the new Microsoft Management Console (MMC) Event Viewer snap-in. Event Viewer is still not a full event log management solution, but it's a much improved tool for casual, ad hoc analysis of security events.

The first thing you'll notice about Event Viewer is the new task pane, shown on the right in Figure 4, page 44, which greatly reduces the clicks required to perform common tasks such as setting up and later clearing a filter. On the subject of filtering your view of the Security log, Event Viewer provides the same basic filter features it's always had but with a number of improvements.

When you click Filter Current Log in the task pane, you'll see the Filter Current Log dialog box shown in Figure 5, page 44. The Logged drop-down box makes it much easier to limit the time range you want to analyze by providing *Last hour*, *Last 12 hours*, *Last 24 hours*, *Last 7 days*, *Last 30 days*, and of course *Custom range* options. These options are a great improvement over Windows 2003 and earlier, which required you to specify exact date and time ranges.

You can limit the view to failure or success events by using the Keywords drop-down box and filter by subcategories with the *Task category* drop-down box. Note that the *Task category* drop-down isn't populated with the 52 audit subcategories until you select *Microsoft Windows security auditing* in the *Event sources* drop-down box. To view the results of your filter, just click OK.

Figure 3: Event ID 529 in Windows 2003

Here's a cool new feature: Once you have the filter set up just the way you want it, you can save it for future use with the Save Filter to Custom View option in the task pane. When the Save Filter to Custom View dialog box appears, you provide a name, a description, and a location under the Custom Views folder (visible in Figure 4).

For the first time, Event Viewer lets you easily attach to events tasks that are automatically executed whenever the events occur. Say you have a special Microsoft SharePoint server dedicated to your company's senior executives, and you want to know whenever an account gets locked out so that you can call the executive and help him or her get back onto the server with minimum inconvenience (for the executive, anyway!). You can trigger a message to be emailed or displayed on the console or a command or script to be executed whenever an account lockout event is logged.

The simplest way to attach a task to an event is to select the desired event in Event Viewer and then click the Attach Task To This Event option in the task pane, which starts the Create Basic Task wizard. The wizard asks you to name the task and prompts you to define the program, email message, or display message you desire when that event ID is logged. After you finish the wizard, you can view the event, its properties, and its history by opening the MMC Task


VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.
VoIP AS YOU ARE.

Let's leave the hardware where it is.

Introducing the software-based VoIP solution from Microsoft. It's a whole new way to look at telephony.

As it turns out, that important move to VoIP isn't about ripping and replacing or big, upfront costs. That's because it's no longer about hardware.

It's actually about software.

That's right. Keep your hardware—your PBX, your gateways, even your phones. Add software. Software that integrates with Active Directory,® Microsoft® Office, Microsoft Exchange Server, and your PBX. Simply maximize your current PBX investment and make it part of your new software-based VoIP solution.

Because what you have is good. What you have with the right software is even better. Learn more at microsoft.com/voip

Your potential. Our passion.™

Microsoft®

Scheduler snap-in found on the Start Menu under All Programs\Accessories\System Tools.

Often, though, you'll need to be a little more specific with your trigger criteria than simply specifying an event ID. The good news is that any criteria you can specify in a custom view filter you can also specify in an event trigger, including advanced filters written in XML. The bad news is that you can't use Event Viewer to create the trigger—you must use Task Scheduler instead. Open Task Scheduler and click Create Task. Specify the name and description of the event as well as what account the task should execute under on the General tab.

Then select the Trigger tab and click New. In the New Trigger dialog box, select *On an event* from the *Begin the task* drop-down list. Select Custom in the Settings drop-down box, and click New Event Filter. Now you're shown the same dialog box as when you create a custom view in Event Viewer. You can either use the Filter tab to specify the filter criteria or use the XML tab to specify an advanced filter in XML syntax. After you finish the trigger criteria, you can go to the Actions tab to specify one or more actions for Task Scheduler to execute.

A final thing I like about Event Viewer is the revamped log retention policy options you see when you open the properties of the Security log. The old *Overwrite events older than _ days* has been replaced by *Archive the log when full, do not overwrite events*, which for the first time exposes a feature that's been around for a long time but was configurable only via the registry by using the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Service\AutoBackupLogFiles setting. If you select the *Archive the log when full* option, Windows will automatically archive the Security log to C:\Windows\System32\winevt\Logs.

A word of caution, though: Windows will continue logging and archiving events until it fills the drive, so you need some kind of automated process for moving the logs. In the end, there's no good substitute for a real log management solution from an ISV. "Event Response," November 2004, InstantDoc ID 44093, compares three such tools. The Security Pro VIP article "Enterprise Event Logging for SMBs," InstantDoc ID 95511, describes six enterprise log collection and management tools.

Get Going

As you can see, a lot has changed and a lot has stayed the same in Windows auditing and security logging, but in general, there are many improvements. The new more granular audit policy will help you eliminate some but not all the noise that Windows writes to the Security log. The automatic task execution capability might help you automate responses or be alerted to important events when they occur. And the custom filter views will certainly help administrators that don't have a full-featured log management solution.

All the new event IDs and their changed formats will definitely mean a steep learning curve and lots of report and alert criteria redesign before you can start monitoring and analyzing Windows 2008 and Vista logs. Ultimately, though, the new formats are an improvement, especially in the area of consistency.

One other major new feature associated with event logs in Windows 2008 and Vista is the new event-forwarding capability, which for the first time allows Windows systems to automatically send events to other servers on which you can theoretically do centralized event management. But collecting logs from multiple computers is a gargantuan task, and Windows 2008's HTTP-based method for event forwarding is only intended for small volumes of events defined with very specific criteria. "Windows Eventing 6.0" describes Windows 2008 and Vista's centralized event-collection capabilities.

Get to know the new event log in Windows 2008 as soon as possible so that your security monitoring and compliance activities can continue unimpaired as you start migrating to the new platform.

InstantDoc ID 96799

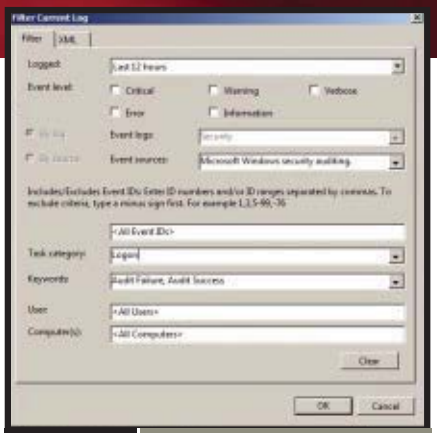


Figure 5: Creating a custom log filter

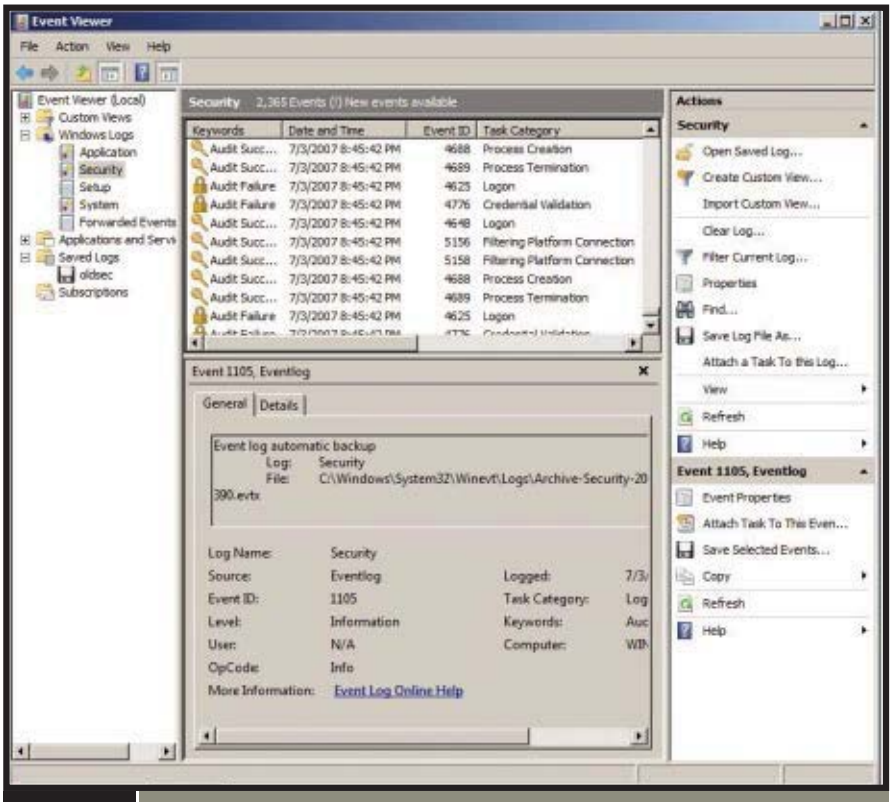
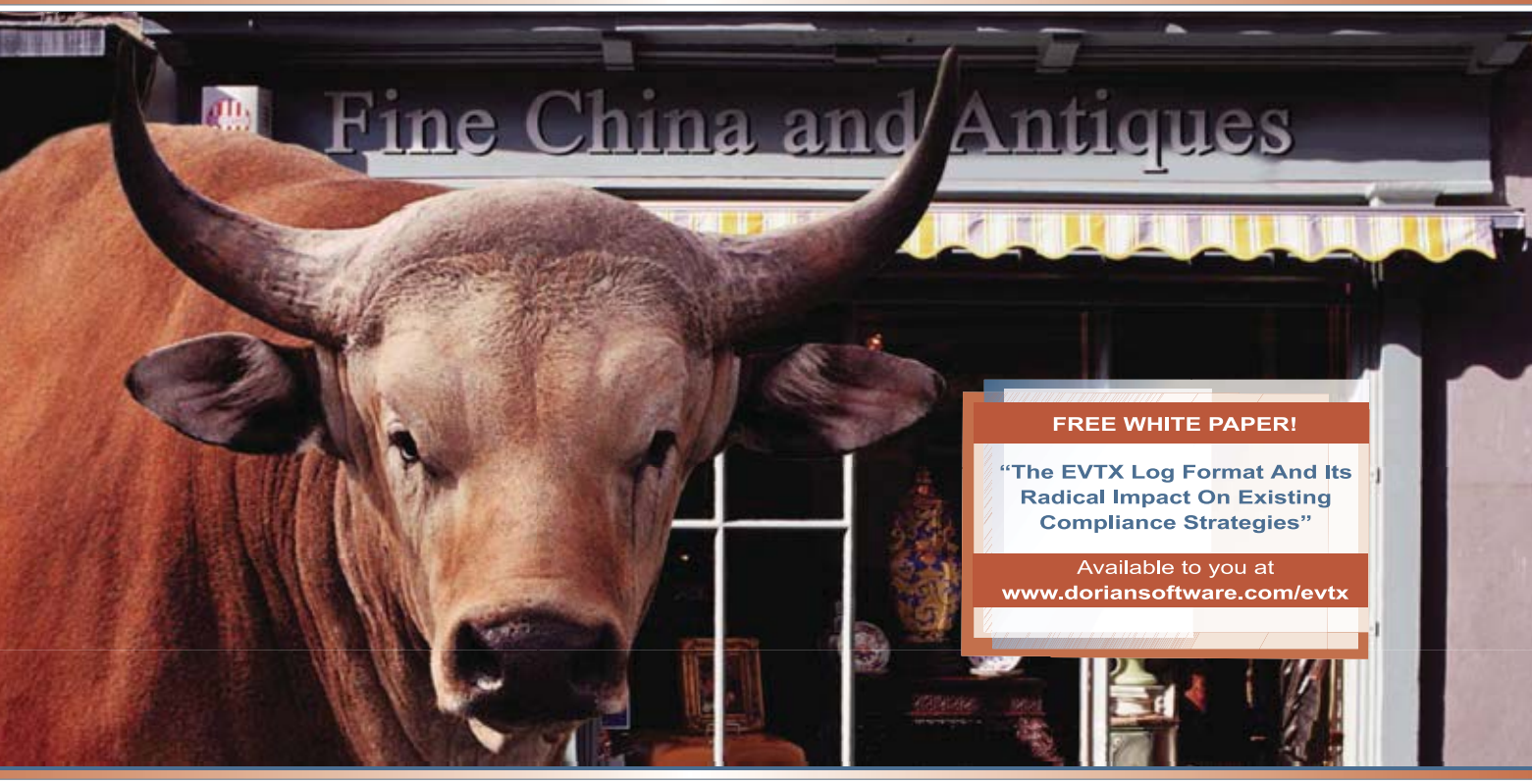


Figure 4: The new Event Viewer with task pane

Randy Franklin Smith
(rsmith@ultimatewindowssecurity.com) is a contributing editor for *Windows IT Pro*, an information security consultant, and CEO of Monterey Technology Group. He teaches Monterey Technology Group's Ultimate Windows Security course series and is an SSCP, a CISA, and a Security MVP.



SERIOUS EVENT LOG MANAGEMENT WITHOUT THE BULL.™

But with Windows Vista™ and Windows Server® 2008 log compatibility . . . for when you are ready.

Now Featuring **LogRefiner™ Technology**

Move to Windows Server® 2008 and Windows Vista™ on your terms!

For years, the Dorian® Total Event Log Management Solution™ has helped organizations meet the expanding log management demands of standards such as Sarbanes-Oxley, HIPAA, and PCI.

Developed, patented, and supported in the USA, our modular approach to log management provides frontline monitoring of the event log and syslog with Event Alarm®, automates the collection of log data with Event Archiver®, and provides reporting via Event Analyst®. Finally, Event Rover® provides additional log data mining capability.

PATENTED

Today, like a bull in a china shop, a shift in the Microsoft Windows® log format threatens to wreak havoc in your compliance and SEM efforts. That's why we've already introduced LogRefiner™ technology - an exclusive approach for a seamless transition between management of older Microsoft Windows log files and the new, expanded EVTX logging format.

Make the move to Windows Vista™ and Windows Server® 2008 at your pace and on your own terms. You can continue to manage existing log files as well as logs in the new format side-by-side and without issue. All the while, the older logs will still be freely available to you for auditing and forensics purposes.

SEM and SIM consoles, overly-complex and costing thousands of dollars per server, aren't required. Factory-sealed appliances or proprietary back-ends are also unnecessary. Instead, let Dorian integrate log management with your existing databases and storage systems, providing easy access to years' worth of log files - whether in EVT or EVTX format. Enjoy the praise for thinking ahead. Look to Dorian for log management without the bull.™

DORIAN®
www.doriansoftware.com

1997 10 YEARS 2007
MANAGING THE EVENT LOG

Event Rover® · Event Alarm® · Event Archiver® · Event Analyst®

www.doriansoftware.com/withoutthebull

FOR FREE WHITE PAPERS AND EVALUATIONS

PowerShell Scripting

BY DANNY KIM

SOLUTIONS SNAPSHOT

PROBLEM:
Managing and archiving Group Policy Objects (GPOs) listed in a Microsoft Excel spreadsheet is a difficult Group Policy task.

SOLUTION:
PowerShell lets you write a simple script to accomplish this task.

WHAT YOU NEED:
Group Policy Management Console (GPMC), PowerShell, Excel

DIFFICULTY:
●●○○○

Back in the '80s, I remember doing everything on a PC inside a black walled window, typing commands into a DOS prompt. Then came Windows and the advent of the GUI. The days of the command prompt appeared to be over, especially for the Windows user. Until now—because a small group at Microsoft has decided to go back to the basics. They created a tool called PowerShell that combines the ease of use of a command prompt, the power of object manipulation, simple but flexible cmdlets, and the ability to easily access Microsoft .NET classes.

Installing and running PowerShell isn't all that exciting on its own, because most people's first commands are the familiar Dir or Cls commands from the DOS days. However, like a Swiss Army knife, the beauty of PowerShell is its ability to solve difficult problems with unbelievable ease. To illustrate these capabilities, we'll tackle a difficult Group Policy management challenge: managing and archiving Group Policy Objects (GPOs) listed in a Microsoft Excel spreadsheet.

I'll use PowerShell to demonstrate how easily you can accomplish this task with just a few lines of code. I chose this scenario because in almost every company I've visited, regardless of whether they use a third-party GPO management tool or the native Group Policy Management Console (GPMC) tool, everyone seems to maintain a list of GPOs (along with their status, change information, owner, etc.) in an Excel spreadsheet. (For more information about PowerShell, see the Learning Path.)

STEP 1: Download and Install GPMC and PowerShell

GPMC is the de facto management console for viewing, archiving, and analyzing GPOs in Active Directory (AD). Although we aren't going use the GPMC Microsoft Management Console (MMC) UI, we do need GPMC's COM automation DLL for our PowerShell script to call its APIs.

GPMC ships only with Windows Vista. If you're running an OS other than Vista, you need to download GPMC from http://www.microsoft.com/windowsserver2003/gpmc. Just install the file GPMC.msi; all the COM registrations are handled automatically and will then be easily accessible from PowerShell.

Next, download the appropriate version of PowerShell for your OS. You can download PowerShell from

	A	B	C	D	E	F	G
1	GPOName	GPOGUID	Domain	Owner	Department	Change Control	Description
2	AsiaBU	{B1711641-6930-48AE-918D-629	Asia	Jason Tan	IT-Asia	Approve	Asian Division Standard GPO
3	EuropeBU	{B1711641-6930-48AE-918D-629	Europe	Scott Johnson	IT-Europe	Approve	Europe Division Standard GPO
4	BranchOffice1	{34774FC3-8F0B-4759-ADAC-3D	Americas	Lynda Ferry	Marketing	Validate	Marketing Branch Office US location GPO
5	BranchOffice2	{BCBBCEB5-C2F0-444F-9DEF-84	Americas	John Fitzgerald	Sales	Validate	Sales Branch Office US location GPO
6							

Figure 1: Sample GPO spreadsheet

Group Policy change management made easy!

http://www.microsoft.com/windowsserver2003/technologies/management/powershell/download.mspx. Notice that PowerShell is supported on Windows XP SP2, Windows Server 2003, and Vista on both x32 and x64 platforms. Before installing PowerShell, make sure you have Microsoft .NET Framework 2.0 installed. The x86 platform version is available at http://www.microsoft.com/downloads/details.aspx?familyid=0856eacb-4362-4b0d-8edd-aab15c5e04f5&displaylang=en (with links on the page to other platforms).

STEP 2: Create a Sample GPO Spreadsheet

Most administrators document their GPOs in some form, whether in an Excel spreadsheet, a database, or even a Notepad file. If you haven't documented your GPOs, now is a good time to start.

As Figure 1 shows, I used four GPOs. My sample Excel spreadsheet describes specific attributes of each GPO, such as GPOName, GPOGUID, Domain, Owner, Department, Change Control status, and Description. You'll need to list the GPOs that exist in your AD, or create test GPOs in your AD for this exercise and update the GPOName, GPOGUID, and Domain columns with your own GPOs that you want to back up. After completing the Excel spreadsheet, save it as a comma-separated value (CSV) file called GPOList.csv.

PowerShell has built-in cmdlets that let you import the contents of a .csv file, then navigate to individual items inside the spreadsheet as objects. This is one of the key differences between PowerShell and typical UNIX shells or other scripting languages such as Perl. Whereas UNIX shells and Perl operate on data as pipes of text to pass forward, PowerShell allows the infinitely more flexible feature of storing and passing object references that can be queried, manipulated, searched, and operated on as collections. PowerShell was originally designed as a .NET scripting language—this underlying infrastructure is obvious in PowerShell's ability to inherit .NET's capabilities for data manipulation, while keeping the technology accessible.

In your sample spreadsheet, you can create any number of columns with any amount of information for each GPO. For consistency, we'll designate the first column as GPOName because that's what we'll use as our unique identifier.

STEP 3: Create the PowerShell Script

We'll start with a PowerShell script that calls GPMC's COM APIs for initiating a GPO backup. Listing 1 contains this code, called BackupGPO.ps1. First, the script creates a reference to the GPMC COM Automation object. In VBScript, you'd call the function CreateObject—for example, Set GPM = CreateObject("GPMgmt.GPM"). PowerShell has an equivalent function called New-Object; passing in the -comobject GPMgmt.GPM parameter, as callout A in Listing 1 shows, initializes the GPMC COM object.

A useful PowerShell feature is that for any cmdlet, parameter, or object, if you enter the first few characters of the cmdlet or parameter and press Tab, PowerShell fills in the closest match. If you continue to press Tab, you'll cycle through all the possible cmdlets, parameters, or object attributes. For example, after you set the $GPM variable at callout A in Listing 1, if you enter $GPM. and press Tab, you'll see all the COM functions that GPMC has exposed.

We also need to grab the constants from the GPMC object and create a variable that can be passed into our COM functions; the code at callout B accomplishes this task. In addition, we need to use the DNS names from the sample .csv file to obtain the domain object GPMDomain via a call to the GetDomain GPMC API;

SOLUTIONS SNAPSHOT

SOLUTION STEPS:

1. Download and install GPMC and PowerShell.
2. Create a sample GPO spreadsheet.
3. Create the PowerShell script.
4. Execute the backup filter.

Listing 1: BackupGPO.psl

```
filter Do-GPOBackup
{
A   $GPM = New-Object -comobject GPMgmt.GPM
B   $const = $GPM.GetConstants()
C   $GPMDomain = $GPM.GetDomain($_.Domain, "", $Const.UseAnyDC)
D   $GPO = $GPMDomain.GetGPO($_.GPOGUID)
E   $GPMResult = $GPO.Backup("C:\\backup", $_.Description)

    Write-host "Backed up GPO $($_.GPOName)"
}
```

the code at callout C accomplishes this task.

Next, we need to call the GPMC API to select the appropriate GPO, as the code at callout D does. Notice that this line of code uses a new operand (i.e., $_.) and specifies the column name of the .csv file we created earlier. The $_ operand lets us access sets of data within each column, stored by PowerShell as .NET objects.

The last line in our GPMC API calls, which callout E shows, is the final call to actually do the backup. In this example, I hard-coded the backup location to C:\backup. This location can be passed in or be part of the columns in the passed-in .csv file. The PowerShell command is

```
$Result = $GPO.Backup ("C:\\backup", $_
  .Description)
```

Note that when you pass in a directory name to a COM-based function call, you need to use two backslashes because single backslashes are interpreted as escape characters. Make sure the directory C:\backup exists before you call the PowerShell script.

Finally, we add a single line of code at the beginning to name our filter and put the code we've written so far in a block to allow objects to be passed in as a filter. Functions are typically created with parameters that are passed in. In our case, the whole .csv file is passed in and we're dynamically accessing all the objects within the file. Using functions doesn't make sense because we aren't specifying static parameters. Filters just take whatever is passed in—the code inside the filter handles and makes assumptions about the data to use.

If we wanted to get more advanced, we could add error checks to make sure the $GPMResult variable is valid and that no exceptions have been thrown, to determine the script's success or failure. However, I wanted to keep the example simple.

STEP 4: Execute the Backup Filter

Now we get to see PowerShell's magic and flexibility. First, start PowerShell and change the PowerShell policy to allow execution of scripts. To do so, enter

```
PS C:\> Set-ExecutionPolicy
  -executionPolicy Unrestricted
```

Next, load the PowerShell code from Listing 1 by "dot-sourcing" the PowerShell file. This action essentially loads the filter we've created into the current PowerShell runspace.

As I already explained, passing a .csv file as a parameter only passes the reference to the .csv file in a function. You then have to write code in the function to manually parse the contents of the .csv file. Passing the .csv file in as a filter lets us access all of the file's data elements as .NET objects inside the filter.

Enter

```
PS C:\> . C:\PSDemo\BackupGPOs.ps1
```

Then, import the .csv file and pass it into the Do-GPOBackup filter we wrote. Enter

```
PS C:\> import-csv C:\PSDemo\GPOList.csv
  | Do-GPOBackup
```

Figure 2 shows the output.

The PowerShell script that we created can take as input any .csv file for performing operations on GPOs. We can also add a parameter check to operate only on GPOs that match a certain domain name. For example, for the domain Americas, enter

```
PS C:\> import-cvs C:\PSDemo\GPOList.csv
  | {where $_.Domain = "Americas"} | Do-
  GPOBackup
```

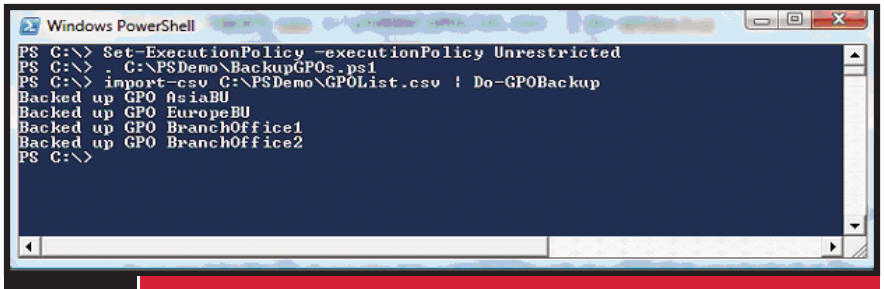


Figure 2: Output from executing the backup filter

Learning Path

WINDOWS IT PRO RESOURCES

"Dig Out By Digging Into PowerShell," InstantDoc ID 96075

"Getting Started with Windows PowerShell," InstantDoc ID 93560

"Introducing Windows PowerShell," InstantDoc ID 50565

"PowerShell One-Liners for Managing the File System," InstantDoc ID 96320

MICROSOFT RESOURCES

Scripting with Windows PowerShell
http://www.microsoft.com/technet/scriptcenter/hubs/msh.mspx

Windows PowerShell
http://www.microsoft.com/windowsserver2003/technologies/management/powershell/default.mspx

Another option is to take the result and pipe it to a graph to identify the GPOs that were backed up, time them to see which ones are taking the longest to back up, and pinpoint which ones are creating the greatest performance problems. The possibilities are now endless. We could modify the PowerShell script so that instead of performing backups, we could perform periodic restores of critical GPOs by scheduling them via Task Scheduler. In addition, simply changing the spreadsheet contents would dynamically change the list of GPOs being operated on, backed up, or restored.

Back to Basics

My simple example demonstrates PowerShell's extreme flexibility. Using this example as a foundation, you can automate the reporting, analysis, creation, and even provisioning of new GPOs. You can also use PowerShell to link GPOs to organizational units (OUs) in AD. Because Microsoft used PowerShell as the back end to write Exchange Server 2007's management UI, you can designate something as simple as an Excel spreadsheet or as intricate as Exchange's management UI as your preferred UI. PowerShell's simple but immensely useful command prompt lets you truly go back to basics.

InstantDoc ID 96827

Danny Kim

(dkim@fullarmor.com) is a Microsoft MVP and an industry expert on Windows Group Policy. He has helped many Fortune 100 companies design and deploy Group Policy infrastructures and has architected several leading Windows policy management products.

30 million computer users don't trust the power grid.

APC **Smart-UPS® 1000** provides power protection and battery backup during power outages. *Also available in rack-mount models.*

They do trust APC. Shouldn't you?

"Overall the reliability of electrical systems in the US almost certainly will decline over the next 10 years."

– Venture Development

Think of all that you rely on your computer for: personal and business files, financial information, broadband access, videos, photos, music, and more. Increasingly, computers are the hub for managing our lives. And more people rely on APC to protect their hardware and data than any other uninterruptible power supply (UPS) brand.

Why is APC the world's best selling power protection? For 20 years, we have pioneered power protection technology. Our Legendary Reliability® enables you to save your data, protect your hardware, and prevent downtime. It also guards against a power grid that is growing less reliable every day.

According to the Department of Energy, electricity consumption will increase by 40% over the next 10 years. Yet today, investment in utilities is at an all-time low. It's a "perfect storm" for computer users, one that makes APC protection even more essential.

APC has a complete line of power protection solutions to suit a range of applications. Already an APC user? Get the latest replacement battery cartridge for your unit or upgrade to a newer model.

Find out why 30 million people don't need to worry about losing their music, photos, and financial files.

Find APC power protection products at: COMPUSA We got it. We get it. CDW Office DEPOT

APC Solutions for Every Level of Protection

Home Starting at **$59.99**

Best value battery backup and surge protection for home computers.

8 outlets, DSL protection, 44 minutes of runtime

Back-UPS® ES 550R

Home Office Starting at **$99.99**

Complete protection for home and small business computers.

10 outlets, DSL and coax protection, 70 minutes of runtime

Back-UPS® ES 750

Small Business Starting at **$459.00**

High-performance network power protection with best-in-class manageability for servers.

Smart-UPS® 1000

Register to WIN a Smart-UPS® 1000 – value $459 ERP.

Also, enter keycode to view other special offers and discounts.

APC® Legendary Reliability®

Visit www.apc.com/promo and enter key code x535x • Call 888-289-APCC x4667 • Fax 401-788-2797

tools4ever

User Account Management automated at CentraState Healthcare

CentraState HealthCare System recently embarked on a project to find a secure and automated method for managing user account lifecycle in Active Directory and Exchange for their employees at six locations. When the search started, CentraState IT staff was managing the process manually utilizing Microsoft Active Directory Users and Computers.

The reasons for automating the process were as follows:

- Seamlessly manage User accounts by linking with the Lawson Human Resource application for new hires and terminations and avoid manual intervention.
- A need for the account name and other relevant information in Lawson.
- Easily create Users in the proper Organizational Unit based on location and department and avoid errors.
- Create email accounts on the proper server/store based on location.
- Immediate disabling of user accounts upon termination for greater regulatory compliance.

CentraState selected the Tools4ever User Management Automation module along with professional services to complete the bi-directional link between Lawson and Active directory.

About the Solution

As employees are hired by CentraState, their pertinent information is entered into the Lawson HR system that currently runs on an IBM *i*-series (AS 400) computer. Conversely, as employees resign, a termination date is placed in the HR system.

On a regularly scheduled basis, the User Management application starts a query to capture all employee data and begin the process of updating Active Directory. If the account already exists in AD, any updates, such as name, location or department changes are appropriately processed. If the account does not exist, it is created along with an Exchange mailbox, home directory and assigned to the appropriate Group Profiles based on job title and department. If the employee start date is in the future, the account is created but put in a disabled state until the date is reached when it is activated.

CentraState's naming requirements for both Active Directory and Exchange mailboxes were handled automatically by the application as were the iterations required, when necessary, for uniqueness. Business logic was also defined within the product to allow the automatic placement of users into the correct OU based upon their specific location and department. This location and department information is also utilized to insure mailboxes are created within the proper server and store. When an employee termination occurs, the information is processed by User Management and accounts are appropriately disabled on the date and then deleted after a specific period of time has passed.

Information that is created during the Active Directory processing, such as User Account Name and e-mail address, is fed back to the Lawson database twice a day. This is done to insure that Lawson is accurate information when anything has changed in Active Directory without requiring manual intervention.

Advantages

Approximately 2 weeks after commencement, the entire project was implemented and operational. The reduction in time spent by the staff managing user account lifecycle was tremendous. Commenting on the project, Mark Handerhan, IT Manager, stated, "*The Tools4Ever implementation was one of the most highly valuable, cost effective solutions that I've ever implemented. We have taken the manual intervention out of the equation for many mundane AD /user tasks, such as disabling network accounts. User accounts are now disabled in real-time once terminated in Lawson. This provides us with a greater level of network security, while also assuring compliance with industry standard regulations such as HIPAA. "* In summary, the IT staff at CentraState can spend more time on mission critical support and planning while eliminating the requirements to spend time on routine user account tasks.

About CentraState

CentraState Healthcare System is a non-profit community health organization consisting of an acute-care hospital, three senior living centers, a health education and activities center, a family medicine residency program, and a charitable foundation. It is a member of the Robert Wood Johnson Health Network and a clinical research affiliate of The Cancer Institute of New Jersey.

About Tools4ever

Tools4ever offers quality and scalable productivity solutions for the Windows 2000/2003 system administrator with the main focus on User Provisioning and Life Cycle management, Identity Management, Active Directory management and employee self service.

Tools4ever, Inc. 516.482.4414 www.tools4ever.com

The Inevitability of IPv6 PART 1

BY JOHN HOWIE

A switch from IPv4 to IPv6 is on your horizon. Are you ready for it?

Internet Protocol version 6 (IPv6) is the set of protocols that will replace today's IPv4. IPv6 offers many benefits necessary to support the Internet's continuing expansion—most notably an expanded address space that overcomes pressures in regions such as Africa, Asia, China, and the Middle East. Temporary solutions such as Network Address Translation (NAT)—although effective in the short term—won't provide long-term help. Recognizing that IPv6 is the future, many governments are mandating that their systems and networks support IPv6, including the US government, which has set a transition date of June 30, 2008. If your company does business with entities that use (or plan to use) IPv6, you'll feel the pressure to support IPv6, if only to support communications between your company and your partners. Simply put, IPv6 might become a competitive advantage.

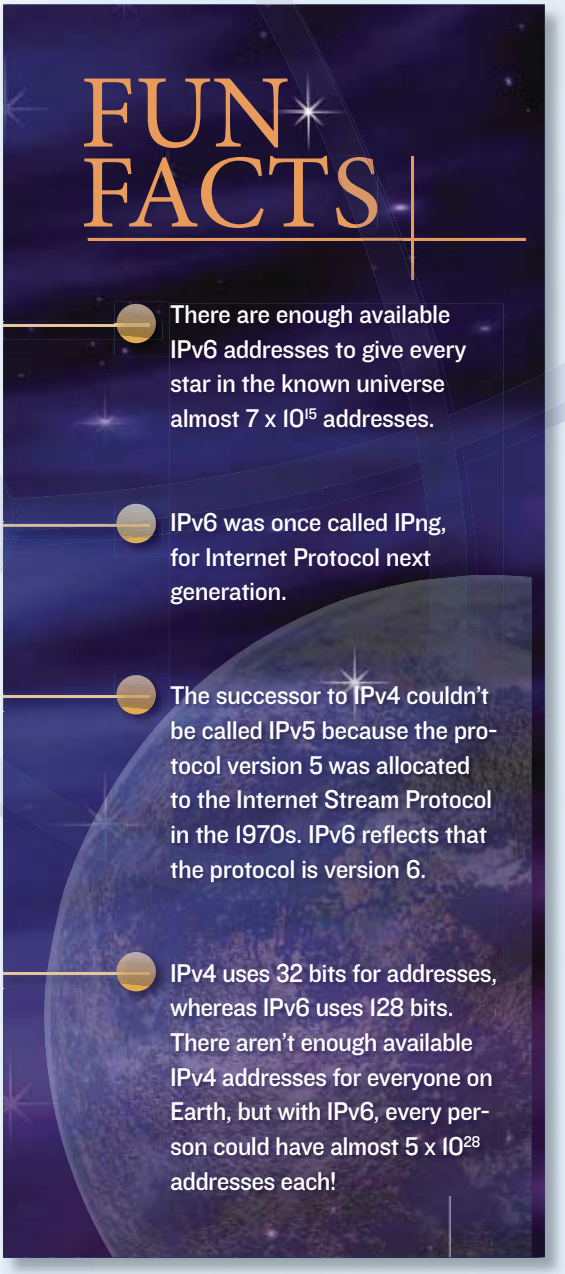


Figure 1: Global Unicast Addressing

In this first part of a three-part series, I describe IPv6 addressing in detail, focusing on how its addressing scheme works. I also describe some of the new features of IPv6, as well as some of the reasons you should care about it—even if you don't plan on implementing it in the near future. In two future articles, I'll describe how to install IPv6 onto Windows Server 2003 and Windows XP, and how to configure interfaces with addresses and enable DNS resolution. I'll also describe in detail how to configure your systems and networks to use IPv6 and IPv4 together while you transition to an all-IPv6 network. Finally, I'll look into strategies for using IPv6 over the IPv4 Internet if your ISP doesn't support IPv6. But first, we need to lay down a foundation.

Windows Support for IPv6

Almost every modern OS supports IPv6 out of the box. In fact, you're probably running IPv6 on your networks without even realizing it. Microsoft supports IPv6 in Windows Vista, Windows 2003, XP SP1 and later, and Windows CE .NET 4.1 and later. Windows Server 2008 will also support IPv6. Microsoft Research produced an IPv6 stack for Windows 2000 and Windows NT, but it isn't supported. To obtain the stack, see the Learning Path online.

Only Vista has IPv6 enabled "out of the box." If you have Vista installed on your network, you're running IPv6. Vista will configure link-local addresses in the absence of IPv6 infrastructure hardware such as DHCP servers, IPv6-capable routers, and so on. Once enabled, XP will function as an IPv6 client, letting you conduct many common communications (e.g., Web browsing using HTTP or HTTPS) over IPv6. Windows 2003 also supports IPv6 in most communications.

IPv6 Addressing

IPv6 gives you a whole new means of uniquely addressing a node (or end system). In IPv6, there are 128 bits available to uniquely identify a node. IPv4 offers 32 bits, for a total of more than 4 billion possible combinations, but far fewer are practically available because of the way address space has been organized.With 128 bits, we'll have sufficient addresses for the next millennium—even given the way addresses are allocated.

Before I discuss the allocation and use of IPv6 addresses, it's helpful to understand the format that's used to represent them. Whereas IPv4 uses a dotted-decimal system (e.g., 192.168.16.10), IPv6 uses a different format. An IPv6 address is split into eight 16-bit blocks: Each block is represented by four hexadecimal digits, and each block is separated by a colon (:)—for example, 2001:0000:0000:e388:0092:fb7f:a827:fad6. Within each block, leading zeroes can be omitted so that the address can be read as 2001:0:0:e388:92:fb7f:a827:fad6. Also, blocks of zeroes can be omitted, so that the address can be further simplified as 2001::e388:92:fb7f:a827:fad6. Note the use of the double colon to represent the blocks of zeroes. If you have more than one block of consecutive zeroes in an address, only one block can be omitted. (Otherwise, it would be impossible to reconstruct the original address.)

Currently, three types of IPv6 addresses can be allocated to a node: *unicast, multicast,* and *anycast.* A unicast address uniquely identifies a single interface (or network connection) on a node (or a virtual interface on clustered systems). A multicast address is similar to an IPv4 multicast address and can be shared by several interfaces on several nodes. A packet with a multicast destination address is delivered to all interfaces on all nodes that share the address. However, a packet with an anycast destination address is delivered to only one interface: the nearest interface to the sending interface. Regardless of type, the address identifies an interface on a node—not the node itself. A node will likely have multiple IPv6 addresses, even if it has only one interface.

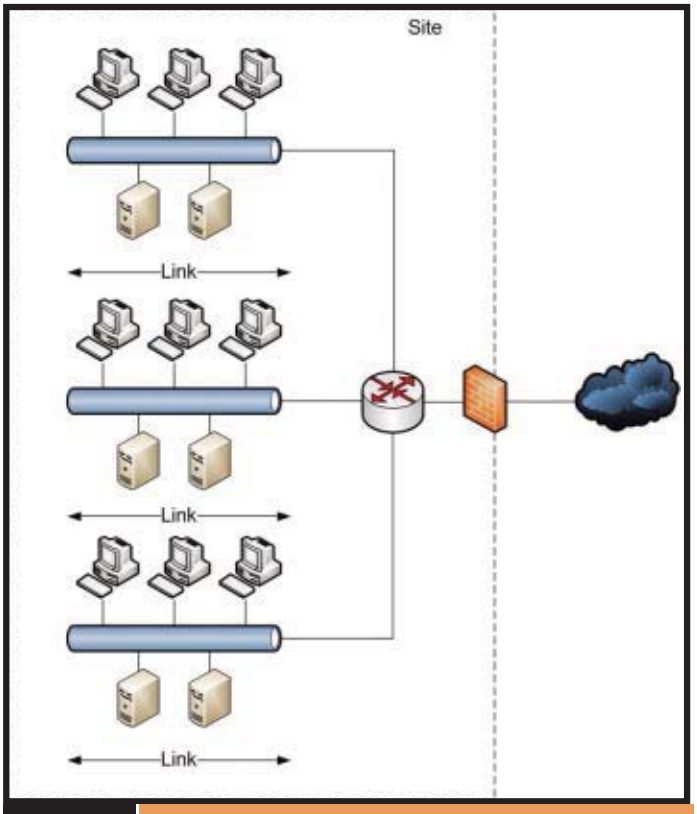


Figure 2: IPv6 Address Scope

Unicast Addresses

Each interface can have more than one unicast address. A unicast address can be an Aggregatable Global Unicast Address (aka global address), or a Local-Use Unicast Address.

Global address. A global address is unique to the interface it's assigned to and can be used to reach that interface from any other interface. Global IPv6 addresses are hierarchical and contain routing information. Figure 1 shows the format of a global address. A unicast address's first three bits—called the Format Prefix (FP)—are always 001. FPs can be of varying length (e.g., the multicast FP is eight bits in length). The next thirteen bits comprise the Top-Level Aggregation Identifier (TLA ID). This ID is allocated to top-level ISPs, of which there can be 8,192.

Next in the address is a reserved field—eight bits in length and designed for future expansion of the TLA ID. The next field in the address, the Next-Level Aggregation Identifier (NLA ID), is 24 bits in length and is used by the top-level ISP to organize networks or to support second-tier ISPs, each of which would have one or more NLA IDs assigned to them.

These combined 48 bits uniquely identify a site belonging to the top-level or second-tier ISP's customer. Sites are determined by geography. For example, an international company might have many sites. Each site's IPv6 connection will have a 48-bit address unique to the site. Each site can use the next sixteen bits in the address—called the Site-Level Aggregation Identifier (SLA ID)—to divide the site into subnets. Each site can have 65,535 subnets. Alternatively, if a company has multiple sites but only one IPv6 connection via an ISP, it can use the SLA ID to route between the sites and to the connection. The last field in the global address is the Interface ID, which is 64 bits in length. This field is similar to IPv4's host identifier, which uniquely identifies the host on the network.

Local-Use Unicast Address. There are two types of Local-Use Unicast Addresses. The first is called a *link-local address*, which is used to communicate between interfaces belonging to nodes on a single link. The second is called a *site-local address*, which is used to communicate between interfaces belonging to nodes in a site. Both are viable alternatives to a global address, depending on the scope. Figure 2 shows the scope of a link and a site.

> IPv6 gives us sufficient addresses for the next millennium.

Link-local addressing is similar to IPv4's Automatic Private IP Addressing (APIPA). Link-local addresses begin with an FP of FE80:—the last 64 bits of a link-local address are the Interface ID, and the bits in between the FP and the Interface ID are zeroed out. As with APIPA, link-local addresses are automatically configured without the need for a DHCP server or manual configuration. In fact, every IPv6-capable interface automatically has a link-local address configured for it. If you have any nodes on your network that support interfaces with IPv6, they'll have a link-local address and might be sending packets onto your network as part of Neighbor Discovery. Two nodes on the same link with interfaces that support IPv6 will automatically be able to communicate with each other, without any further configuration or management. However, communication using link-local addresses is restricted to a link—IPv6-aware routers should never forward packets with link-local source or destination addresses.

Site-local addresses are similar to the IPv4 private addresses, which have the network identifiers 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. Site-local addresses always begin with an FP of FEC0:. As with link-local addresses, the last 64 bits of the address com-

prise an Interface ID. The lower 16 bits of the top 64 bits—called the Subnet ID field—uniquely identify subnets in the site, the same as the SLA ID field in a global address. The bits between the FP and the Subnet ID field are zeroed out.

IPv6 uses two special constant addresses. The first is called the *unspecified address* and is always set to 0:0:0:0:0:0:0:0, or just :: for short. This address—similar to the IPv4 address 0.0.0.0—functions as a source address when no other address is available (e.g., when requesting an IP address from an IPv6-capable DHCP server). The second address is the *loopback address* and is always 0:0:0:0:0:0:0:1, or simply ::1. This address—equivalent to the IPv4 loopback address 127.0.0.1—can be used for local testing of applications and configuration. Every interface will respond to the loopback address.

The Interface ID

The Interface ID in a unicast address is always 64 bits in length. It was designed this way to support 48-bit MAC addresses of current 802.x LAN technologies such as Ethernet, and wireless technologies such as Bluetooth and Wi-Fi, as well as the 64-bit addresses that FireWire uses. Future 802.x series LAN and wireless technologies will also use 64-bit addressing. The requirement to support 48-bit and 64-bit MAC addresses comes from the requirement that the Interface ID in a unicast address can be derived from a MAC address using an Extended Unique Identifier (EUI) 64 address. The Interface ID can also be assigned manually or by an IPv6-capable DHCP server.

In the most common scenario, the Interface ID is derived from the 48-bit MAC address of an Ethernet card. A 48-bit MAC address is split into two 24-bit halves. The IEEE assigns the first 24 bits to manufacturers. The manufacturer uses the second 24 bits to uniquely identify the card. Although it's possible to override the MAC address of an Ethernet card, let's assume that it hasn't been overridden. To convert a 48-bit MAC address to a 64-bit Interface ID, the system first copies 24 bits of the MAC address to the first 24 bits of the Interface ID. Bits 17 and 16 of the first 24 bits representing the manufacturer (reading from right to left, starting at 0) are always set to 00. During the copy, the system sets them to 10. After the 24 bits are copied over, 16 bytes are added, and they're always 0xFFFE. The system then copies 24 bits in the second half of the MAC address to produce the 64-bit Interface ID.

In dial-up scenarios, the Interface ID can be generated using a process designed to guarantee the anonymity of the user. If not for this provision, a system could be tracked as it used the Internet, regardless of the ISP used, because the Interface ID would be unique to the computer regardless of the ISP.

Multicast Addresses

IPv6 multicasting is similar to IPv4 multicasting. A node that wants to listen for multicast traffic will set the IPv6 address of an interface to the multicast address that the traffic is being sent to. Multicast addresses have an FP of 0xFF. The next four bits of the multicast address comprise the Flags field. The lowest bit in the Flags field is called the Transient flag. If set to 0, the multicast address is a well-known address set by IANA; if set to 1, it's a non-permanent or transient multicast address. The next four bits of the multicast address comprise the Scope field. The purpose of this field is to identify the scope of the multicast traffic, and to identify the traffic as node-local, link-local, site-local, organization-local, or global. Routers use this field to determine whether to forward traffic. The last field in the multicast address is the Group ID, which is 112 bits in length. The Group ID identifies the multicast group. As with unicast addresses, there are predefined multicast addresses. Table 1 lists the three most common ones.

Table 1: Common Predefined Multicast Addresses

Multicast Address	Use
FF01::1	Node-local scope for all nodes
FF02::1	Link-local scope for all nodes
FF05::1	Site-local scope for all nodes

> There's more to IPv6 than simply an expanded address space.

When using multicasting in IPv6, you should use only the bottom 32 bits of the Group ID field and zero out the top 80 bits. Doing so eases conversion support of the multicast address to an Ethernet multicast address. An Ethernet multicast address takes the form 33:33:xx:xx:xx:xx. Using the recommended multicast addressing format, the bottom 32 bits of the Group ID create the Ethernet multicast address.

IPv6 also uses multicast addresses to support link address resolution. Every interface adds a multicast address for each of its unicast addresses. The multicast address takes the form FF02::1:FFxx:xxxx. The system copies the last 24 bits of the unicast address to the multicast address to replace the xx:xxxx. The system then maps the IPv6 multicast address to the MAC multicast address, as described above. This scheme reduces the number of nodes that have to process address-resolution requests. In IPv4, when one node wants to obtain another node's interface MAC address, the system sends a broadcast message to the broadcast MAC address. Therefore, every interface on the link is forced to process the request—even if it's not intended for it. In IPv6, a node that wants to find another node's interface MAC address will send a broadcast message to the multicast address FF02::1:FF:xx:xxxx, where xx:xxxx is the bottom 24 bits of the interface ID. This, in turn, is translated into a MAC multicast address 33:33:FF:xx:xx:xx. Only those interfaces on the link with matching lower 24 bits in their Interface ID need to respond to the address-resolution request.

IPv6 Features

There's more to IPv6 than simply an expanded address space. IPv6 includes a new header format, improved support for extensions and options, flow-labeling capabilities, and authentication and privacy capabilities.

New header format. IPv6's new header format minimizes the overhead often spent processing fields or information in packet headers. In IPv4, routers and end systems are required to examine packets in detail, looking for information necessary to determine whether the packet should be processed further. With IPv6, you'll now find those fields (when required) after the main packet header in Extension Headers. The new header format makes header processing much more efficient at routers, which can

ignore information in any Extension Headers—with the exception of a Hop-by-Hop Extension Header, which must immediately follow the IPv6 header. The Hop-by-Hop Extension Header might contain information necessary for a router, such as a warning that a packet is a Jumbo packet (greater than 65,535 bytes), or that a router must perform additional processing on the packet.

Improved support for extensions and options. The change in the IPv6 packet header format and the use of Extension Headers facilitate this new feature. Options in Extension Headers have fewer limitations on size than in IPv4, and IPv6 is extensible by adding more defined Extension Headers over time. In IPv6, if a destination node receives an IPv6 packet containing an Extension Header that it doesn't recognize, it informs the source node via Internet Control Message Protocol version 6 (ICMPv6) that it can't process the packet. This feature lets nodes implement IPv6 extensions independently of each other and still communicate.

Flow-labeling capabilities. IPv6 uses flow labeling for Quality of Service (QoS). Flow labeling lets a source node define a priority (e.g., real time), which might be used in Voice over IP (VoIP) or video-over-IP solutions to guarantee delivery of a packet within a certain time window. In IPv4, QoS often requires a router or node to look beyond a packet's header for information. In IPv6, all necessary information is in the header.

Authentication and privacy. IPv6's authentication and privacy capabilities are, essentially, IPSec. IPSec is now a requirement in IPv6 implementations, whereas in IPv4 it's an optional component. IPSec supports Authenticated Headers, which authenticate nodes to each other and ensure the integrity of data exchanged between them, and Encapsulating Security Payload (ESP), which has similar functionality but also includes the ability to encrypt data for confidentiality.

Unlike IPv4, in which different implementations of the protocol by different vendors could—and would—result in an inability of nodes to communicate with each other, in IPv6 interoperability is almost guaranteed, thanks to the underlying standards.

Stay Tuned

We've only just started. Now that you've got some solid foundational knowledge about IPv6, you're primed to dive into the actual installation and use of the protocol. Get ready to make it work on Windows 2003 and XP, and prepare yourself for configuring interfaces with addresses and enabling DNS resolution. In a later article, I'll also describe talk about enabling IPv6 and IPv4 interoperability on your way to an all-IPv6 network.

InstantDoc ID 96880

John Howie

(jhowie@microsoft.com) is the director of the World Wide Services and IT Technical Community for Security at Microsoft. He has more than 15 years of experience in information security and is a CISA, a CISM, and a CISSP.

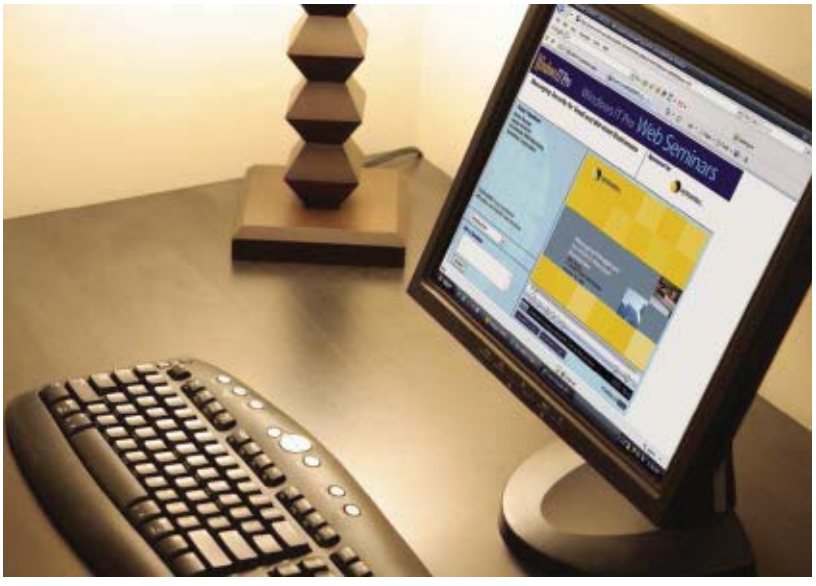
What's Happening at *Windows IT Pro*?

Don't miss the opportunities offered this Fall. With all of the live events, new white papers, web seminars, podcasts, and eBooks available this month, all the information you need is just a click away. To see all that's happening, go to www.windowsitpro.com.

On-Demand Web Seminars

Risk Mitigation for Microsoft Exchange 2007
www.windowsitpro.com/go/ca/ad

11 Reasons to Upgrade to Backup Exec 11d from Symantec
www.sqlmag.com/go/symantec/Exec11d/ad



It's Time To Deploy!

Get the facts about Microsoft Unified Communications and Exchange Server 2007 at one of six day-long workshops starting in mid-October. Don't miss out on your chance to attend in one of the following cities:

- **Portland**
- **San Diego**
- **Denver**
- **Philadelphia**
- **Atlanta**
- **Chicago**

Visit our website for more dates and details at **www.windowsitpro.com/roadshows**

Did You Know...

- 38 white papers await you
- 37 eBooks are waiting to be read
- Why listen to the radio? 22 Podcasts are available
- You are invited to 61 Web Seminars

All just a click away at www.windowsitpro.com

Windows IT Pro

A Trip to the Store with Exchange 2007

New features—and a farewell to some outdated ones—improve the Information Store's stability and performance

by Tony Redmond

The Information Store is the heart of Microsoft Exchange Server. Without a healthy Store, you don't have a successful Exchange deployment, and users are unhappy because they can't access their mailboxes. Exchange Server 2003 and Exchange 2000 Server introduced the concept of storage groups (SGs) and introduced new Store components such as the streaming database. Although the biggest change to the Store in Exchange 2007 is support for the Windows 64-bit platform, Microsoft has made other fundamental changes to the Store that you should also know about when planning your Exchange 2007 migration.

ILLUSTRATION BY TODD DAVIDSON/IMAGES.COM

No SQL Server?

The biggest change that many expected to occur in Exchange 2007 was a transition to Microsoft SQL Server as the database engine for the Store. However, when the Exchange developers investigated the challenges of forcing a database engine designed for structured transactions to handle the work generated by Exchange and its clients, they decided they couldn't do it for Exchange 2007. This isn't altogether surprising when you consider the vastly different types of messages that flow through Exchange—everything from small 2KB messages to multimegabyte messages containing several attachments sent to large distribution lists. Also, users interact with Exchange in ways that affect the database. For instance, Microsoft Outlook users can click a heading in their Inbox to sort messages by that column. This action creates a new custom view in the database. If you consider that a server supports thousands of clients and each client can create many different views, you can sense why the transition to SQL Server could be such an engineering challenge.

The net result is that Exchange 2007 continues to use the Extensible Storage Engine (ESE) that it's used since 1996. Of course, each release of Exchange has modified ESE in different ways, and Exchange 2007 is no different; its major change is the move from a 32-bit platform to a 64-bit platform.

What 64-Bit Means for Exchange

The move to 64-bit is a big plus for Exchange because it addresses some fundamental Store problems in Exchange 2003 and Exchange 2000. For example, as Microsoft releases new versions of the OS, Windows servers gradually use more kernel mode memory to accommodate drivers, such as those used by antivirus and antispam products, and to handle the demand for connections from clients. Five years ago, users typically connected with just a desktop client, so administrators could easily figure out how many concurrent clients a server had to handle based on the number of users whose mailboxes the server hosted. Now, the proliferation of mobile devices means that people use multiple ways to connect to their mailbox. Research in Motion's (RIM's) BlackBerry is popular with many Exchange organizations, but it requires the expense of an additional server infrastructure, so organizations often restrict the use of BlackBerry devices. Microsoft's introduction of server-side ActiveSync (which is less expensive because it uses the same server infrastructure) and the growing popularity of Windows Mobile devices, especially the upgraded functionality delivered by the combination of Exchange 2007 ActiveSync and Windows Mobile 6.0, mean that Exchange 2007 will need to support even more mobile devices in the future. Each concurrent client connection requires memory, so you can see how demand increases.

Virtual memory fragmentation has been a bugbear for Exchange for years, especially in clustered systems. Applications request memory from Windows, which allocates the memory in chunks. Some applications require contiguous chunks of virtual memory to perform operations; if enough contiguous memory isn't available, the application fails. For example, Exchange requires relatively large amounts of contiguous virtual memory to load an SG and mount its databases. When failures occur on a cluster, the cluster attempts to transfer the SGs from the failed node to the other nodes in the cluster, but if enough virtual memory isn't available, the cluster can't transfer the SG, and users lose access to their mailboxes.

The huge increase in available memory made possible by 64-bit Windows OSs relieves the memory fragmentation problems that Exchange 2003 and Exchange 2000 have while also letting Exchange cache much more data than before. The advantage of caching more data is that Exchange 2007 trades expensive disk I/O for memory, which addresses another major performance bottleneck that Exchange suffers on the 32-bit platform. Microsoft predicts that the net effect reduces the I/O operations per second generated by users from around the 1.0 level to about 0.4 (your mileage will vary depending on the exact workload, CPU, and storage configuration). Reducing I/O demand lets you support more concurrent users, but it also requires you to equip Exchange 2007 servers with far more memory than you'd typically deploy with Exchange 2003. Exchange 2007 Mailbox servers with 8GB or more memory will be common, so you'll have to pay attention to the type and speed of memory DIMMs that you specify for servers as you deploy Exchange 2007.

Internally, Microsoft has made other changes to make the Store more efficient. Database pages are now 8KB instead of 4KB, which lets Exchange stuff more data into each page and so generate fewer I/O operations. The Exchange 2007 Store is smarter at write operations and groups transactions together so that single writes occur instead of multiple writes. Finally, the Store makes better use of memory to cache commonly accessed folders and information, such as calendars, to speed user performance.

The change to the database page size and other internal changes mean that you can't mount an Exchange 2003 database on an Exchange 2007 server and vice versa. Because of the complexities involved in an upgrade, Microsoft doesn't support upgrades from a server running 32-bit Windows and Exchange 2003 or Exchange 2000 to 64-bit Windows and Exchange 2007 (even on the same 64-bit–capable hardware), so you won't find a special mode of Eseutil or any other utility to upgrade a database. To move mailbox data from Exchange 2003 or Exchange 2000 to Exchange 2007, you'll have to use the Move Mailbox wizard or the Move-Mailbox cmdlet. Fortunately, you can now script mailbox moves by using Exchange Management Shell to automate these operations. For more information about moving mailboxes, see the Exchange & Outlook Pro VIP article "Exchange 2007: Life Without ExMerge?" January 9, 2007, InstantDoc ID 94629.

Although production Exchange 2007 servers can run only on 64-bit Windows, Microsoft has made a 32-bit version of Exchange 2007 available for use just on test servers. You can also deploy the Exchange 2007 management components, including Exchange Management Shell, on 32-bit Windows XP SP1 workstations (you'll have to install Windows PowerShell and the latest version of the Microsoft .NET framework first). Support for Windows Vista workstations will be added in Exchange 2007 SP1, which is currently in beta and expected to be available by the end of 2007.

Learning Path

WINDOWS IT PRO RESOURCES

For more information about Exchange Information Store databases:

"Back to the Future with Storage Groups," InstantDoc ID 96146

"How Big Is 'Larger'?" InstantDoc ID 93947

For more information about Exchange 2007 clustering:

"MNS and CCR," InstantDoc ID 96245

"MNS and CCR, Part 2," InstantDoc ID 96307

"SCR in the Spotlight," InstantDoc ID 96372

For more information about public folders and SharePoint:

"Migrating Public Folders from Exchange to SharePoint," InstantDoc ID 50172

"SharePoint and Public Folders, Part I," InstantDoc ID 92930

"SharePoint and Public Folders, Part 2: Migration Options," InstantDoc ID 93127

"How SharePoint Matches up to Public Folders," InstantDoc ID 96139

MICROSOFT RESOURCES

"Understanding the Exchange 2007 Store" http://technet.microsoft.com/en-us/library/bb331958.aspx

"Managing Storage Groups and Databases" http://technet.microsoft.com/en-us/library/aa998926.aspx

"Lost Log Resilience and Transaction Log Activity in Exchange 2007" http://technet.microsoft.com/en-us/library/bb288910.aspx

"How to Configure the Transport Dumpster" http://technet.microsoft.com/en-us/library/aa997963.aspx

"Local Continuous Replication" http://technet.microsoft.com/en-us/library/bb125195.aspx

"Cluster Continuous Replication" http://technet.microsoft.com/en-us/library/bb124521.aspx

"Managing Public Folders" http://technet.microsoft.com/en-us/library/bb124411.aspx

Maximum Databases

Every previous Exchange version has imposed a maximum database size on Standard Edi-

tion. Before Exchange 2003 SP2, the maximum database size was 16GB; SP2 increased this to 75GB, a limit that was still too small given the pace of growth in message volume and average message size. By comparison, Exchange 2003 Enterprise Edition supports database sizes that are limited only by available disk space. Some organizations run databases as large as 300GB, but the vast majority of Exchange databases are less than 50GB, largely because of the time required for backup and restore operations. Exchange 2007 doesn't restrict database sizes, so even with Standard Edition you can grow databases as large as you need to. However, Standard Edition is restricted to 5 mailbox databases and 5 SGs, whereas Enterprise Edition can support up to 50 databases and SGs.

You can still deploy up to five databases in a single SG, but Microsoft recommends that you deploy just one database per SG in Exchange 2007. This recommendation is partly to accommodate easier management, partly to provide better performance, and partly because you can only use log shipping to protect SGs that hold one database.

Transaction Logs and Replication

One of the more interesting changes that Microsoft made in Exchange 2007 is to reduce the size of transaction logs from 5MB to 1MB. Transaction logs capture details of every change made to databases in an SG; a busy server can generate tens of gigabytes of log data daily. The size change was made to accommodate log shipping, the mechanism introduced in Exchange 2007 to replicate databases to a location on the same server (local continuous replication—LCR) or to another server in a Majority Node Set (MNS) cluster (cluster continuous replication—CCR). Microsoft announced its intention to expand this functionality to accommodate database replication to a standby server in a different data center (standby continuous replication—SCR) in Exchange 2007 SP1. Log shipping is an important competitive step for Microsoft because IBM Lotus Notes, the company's major competitor in the enterprise market, has supported database replication for many years. It's also a feature that customers have demanded because they don't want to buy third-party products, such as Double-Take, to get similar functionality.

You can use log shipping only for SGs that hold a single database, which is an important consideration for system designers when planning a server's database layout. However, an Exchange 2007 Mailbox server can host up to 50 SGs, all of which can be replicated, so a great deal of flexibility exists. CCR can be used only for Mailbox servers, but you can deploy LCR on multirole servers such as those that support the Mailbox, Client Access, and Hub Transport roles. CCR and LCR don't support public folder databases directly, but Microsoft enables replication by supporting an SG that contains the only public folder database in the organization. If you have more than one public folder database, you can use regular public folder replication to ensure that multiple copies of public folder data exist within the organization.

When you enable an SG for database replication, Exchange "seeds" a passive copy of the database by copying the live database to the location where you want to host the copy (on

the local server or another server). After seeding is complete, Exchange copies and validates transaction logs as the Store generates them, then replays the data in the logs to update the passive copy. If a failure occurs, you can replace the active copy with the passive copy of the database and continue operations. As storage vendors gain experience with Exchange 2007, it's likely that we'll see broader and deeper support for features such as database seeding and log shipping incorporated into third-party storage management products.

Reducing the size of the transaction log exposes Exchange to less risk of losing data due to incomplete file copies caused by a hardware failure. Clearly, you'll lose less data if Exchange can't copy a 1MB transaction log than if it can't copy a 5MB log. Exchange 2007 also includes a new feature called lost log resilience (LLR), which lets Exchange mount databases after a failure even if some data in transaction logs is missing (because of copy failures) and so can't be used to bring a database up to date. LLR runs on CCR Mailbox servers and is a major change for the Store; all previous Exchange versions require manual intervention by administrators if missing data caused the Store to refuse to mount a database. Typically, administrators have to run Eseutil to patch the database. Any manual operation is prone to error, and there are many horror stories where administrators have run Eseutil with the wrong command switches or attempted to apply the wrong set of transaction logs and caused major problems for a database.

Log shipping doesn't happen free of charge; servers incur a performance penalty to copy and replay logs into the passive copy of the database. Read and write I/O operations occur as Exchange copies transaction logs from the active location to an "inspector" directory, where Exchange checksums each log to ensure its integrity before replaying its content into the passive database. Memory is also consumed because Exchange uses a separate ESE instance to replay the transactions. Overall, early experience indicates that you can expect a 20 percent overhead to accommodate these operations on a server that supports LCR. With CCR, the passive node incurs the performance penalty because it pulls logs from the active node and replays them into its copy of the database.

The transport dumpster, another feature introduced in Exchange 2007, further reduces the risk of losing data by caching copies of messages on Hub Transport servers that go to mailboxes in replicated databases. When a failure occurs, Exchange can resend messages from the cache to affected mailboxes. Exchange suppresses the messages if they already exist in the destination mailbox. The transport dumpster can't cache some transactions, such as draft messages, but between log shipping, LLR, and the transport dumpster, Exchange 2007 is more resilient to hardware failure than any previous release.

A minor but important change associated with the smaller log size is the change in transaction log naming. Exchange 2007 still uses the SG prefix to identify the SG that a log belongs to (e.g., all logs beginning with "E0" belong to the first SG on a server), but Microsoft increased the hexadecimal number used to identify an individual log from six to nine characters, so you end up with names such as E010000aa15.log. Microsoft says you can now create more than 4 billion transaction logs per SG before Exchange is forced to reuse a log name.

Portability

Exchange 2007 databases are portable. In other words, you can take a database from a server and mount it on any other Exchange 2007 server in the same organization—something you couldn't do before. Portability helps with disaster recovery because it lets you quickly transfer databases from a failed server and mount them on another server, providing that you can still access the database files. The ability to access the database files to move them is a good reason why shared storage is still an important component in Exchange disaster-recovery planning: It's obviously much easier to switch databases between servers in a SAN than it is if the databases are on direct attached disks.

After the databases are mounted on the new server, you use the Move-Mailbox cmdlet with the -ConfigurationOnly switch to update the configuration data that's stored in Active Directory (AD) for the mailboxes that belong to the databases you just moved and redirect users to the server where the databases are now mounted. Portability is a welcome feature.

Deleted Items

Microsoft introduced the deleted items cache in Exchange Server 5.5 to let administrators avoid restoring databases to recover items deleted in error. The feature has been around for a while and is well understood; the only thing that has changed in Exchange 2007 is that the new default deleted-items retention period is 14 days (instead of 7 days). The deleted-items retention period dictates when the Store permanently removes items from databases, so the change means that Exchange 2007 keeps deleted items for twice as long as Exchange 2003 does. This longer retention period means an increase in database sizes, possibly up to 10 percent depending on user behavior and the flow of message traffic in your organization.

The End of Streaming

Exchange 2000 introduced the streaming database (.stm) file as a companion to the regular Messaging API (MAPI) property database (.edb) file. .Stm files let Exchange store any information that arrived in raw Internet format, such as MIME-encoded messages and attachments, in a database purposely designed to support these formats instead of using MAPI properties in the .edb. Behind this decision was a belief that Internet formats would become much more prevalent than they have and that Exchange could avoid the performance hit of converting MAPI data when IMAP or POP clients such as Outlook Express fetched messages. Since Exchange 2000 appeared, server performance has increased dramatically, so the performance hit for format translation isn't all that important now. Outlook continues to be the most popular Exchange client by far, so MAPI remains the predominant format in use today. Microsoft therefore concluded that the .stm file was no longer needed and omitted it from Exchange 2007.

No More M Drive

The ability to map Exchange mailbox data as a DOS drive using the Server Message Block (SMB) protocol through the Exchange Installable File System (ExIFS) was another feature that received much hype when Microsoft launched Exchange 2000. On the surface, it seemed great that you could navigate through your mailbox as if you were moving through DOS folders.

Unfortunately, the feature turned out to be useless in production, and it even created a host of problems when administrators thought they could virus-scan messages and attachments through the M drive, or when they attempted to take file-level backups of Exchange data through the M drive! Of course, these backups were useless because they didn't contain all the necessary data (such as MAPI properties) that Exchange required, but no one discovered

the problem until a server outage occurred and the backup was needed. Microsoft took the first step to eliminate the problem by hiding drive M by default in Exchange 2003 and now has completed the process by removing ExIFS from Exchange 2007.

Public Folders

Sometimes it seems Microsoft doesn't quite know what to do about public folders. At first, Microsoft deprecated their use in Exchange 2007 with an eye on eventually phasing out public folders completely in the next major release of Exchange. Although public folders aren't the most useful storage mechanism and have never realized the potential Microsoft promised when they appeared in Exchange 4.0, there's no doubt that there are millions of public folders in daily use across the Exchange installed base. Customer push back and the harsh realization that there's no good migration path for public folder data or the applications that depend on public folders forced Microsoft to rethink its decision. The company's latest position is that it will support public folders until 2016 at least.

Having nine years to think about what to do with your public folders is great, but don't expect to see much development around them in the future. You need to start developing an exit strategy. Microsoft will point you to SharePoint, and that's certainly one option, albeit one that requires a lot of manual effort because Microsoft has no automated migration utilities. Quest Software shipped Public Folder Migrator for SharePoint (http://www.quest.com/public-folder-migrator-for-sharepoint), and you can expect other companies to provide utilities over time.

Exchange 2007 includes no GUI to manage public folders, nor does Outlook Web Access (OWA) 2007 include a GUI to access public folders. However, Microsoft will fix these omissions in Exchange 2007 SP1, and you can keep Exchange System Manager around to manage public folders until SP1 appears. Alternatively, you can learn the PowerShell commands to manage public folders and forget about the GUI.

Enhancing the Heart of Exchange

Administrators should find the Exchange 2007 Store changes an improvement. The move to 64-bit Windows improves stability and performance, log shipping increases resilience, and some obsolete components are gone. You can manage the Store by using commands through Exchange Management Shell. There are some outstanding issues, such as the lack of support for public folders in the GUI and OWA, but Microsoft is working to fix these problems in SP1. Features such as log shipping will take time for administrators to learn how to deploy and use effectively, but they're a good step forward. Overall, Microsoft has done a nice job of enhancing the heart of Exchange 2007.

InstantDoc ID 96731

Tony Redmond

(exchguru@windowsitpro.com) is a contributing editor for *Windows IT Pro*, a senior technical editor for Exchange & Outlook Pro VIP, vice president and chief technology officer for HP Services, and author of *Tony Redmond's Guide to Microsoft Exchange Server 2007* (Digital Press).

It's Time to Deploy! Microsoft Unified Communications

Imagine delivering real-time messaging, voice, and conferencing to your desktop environment.

Finally – one solution that bridges the gap between telephony and computing!

Learn how you can benefit from having one solution to manage all of your end users' communications requirements – email, voice mail, calendar, contacts, instant messages and more.

Join us for expert-led tutorials to learn practical, real-world knowledge on how to deploy, manage, and secure Exchange Server 2007 and Office Communications Server 2007.

Portland, OR: October 25
Philadelphia, PA: October 30
Denver, CO: November 6
San Diego, CA: November 8
Chicago, IL: November 15
Atlanta, GA: December 4

What You Will Get:

- *Technical content presented by independent unified communications experts*
- *Timely information from Microsoft about Exchange Server releases*
- *12-month free print subscription to Windows IT Pro magazine*
- *Third-party tools and solutions from key Exchange vendors*
- *Face-to-face access to unified communications experts*
- *Interactive demo area where you can view and handle unified communications devices, such as web cameras, telephones, web conferencing and more*

Who Should Attend?

- *Desktop administrators*
- *Network and system administrators (telephony)*
- *IT generalists*
- *Helpdesk support*
- *IT directors/managers responsible for Exchange migration projects and software upgrades*

Now is the time to learn best practices for real-world application of the unified communications platform.
Register today! www.windowsitpro.com/go/ucflyer

Planning Your Vista Deployment with BDD

Free downloadable tools make your upgrade easier

Rhonda Layfield
(rhonda@minasi.com) is a consultant and trainer.

When you deploy Windows Vista, which of your applications and hardware devices will survive the upgrade? Before you spend a lot of time and money answering that question, check out the free downloadable tools from Microsoft you can use to help your Vista upgrade go smoothly. You can use Microsoft's new Solution Accelerator for Business Desktop Deployment 2007 (BDD) to download tools that help you determine which of your existing computers can be upgraded to Vista and which cannot. The Windows Vista Hardware Assessment (WVHA) tool gathers hardware and software inventory from your entire network. Windows Vista Upgrade Advisor 2.0 (WVUA) reports hardware and software inventory from a single computer. And the Application Compatibility Toolkit 5.0 (ACT) helps troubleshoot applications that don't run properly in Vista.

Let's look at how to install and run these tools. I zero in on creating an inventory, analyzing reports, and the importance of testing your applications on Vista. For a quick reference, see the sidebar "Steps for Preparing for Vista Deployment," page 64.

Installing BDD

Installing BDD requires Microsoft Management Console (MMC) 3.0, which ships with Vista. So, if you're installing BDD on Windows XP SP2, first download and install the MMC 3.0 update from Microsoft (http://support.microsoft.com/kb/907265). Then download BDD (http://www.microsoft.com/downloads). WVUA is a separate download, also available from the Microsoft download center. You must ensure that the version of BDD and its tools match: If you're using the beta version of BDD, you must have the beta version of the tools; if you're using the RTM version of BDD, you need the RTM version of the tools.

Once you have BDD installed, add the components you'll use for the planning phase of your deployment project. Open the Deployment Workbench from Start, All Programs, BDD 2007. Then expand Information Center in the tree pane, as Figure 1, page 64, shows. You'll highlight Windows Vista Hardware Assessment in the Components pane and click the Download button that appears in the Details pane. Perform the same steps for the ACT. After the toolsets are downloaded, they will appear in a list in the Downloaded section of the Components pane.

WVHA scans and inventories your networked computers by using Windows Management Instrumentation (WMI) calls, so no agents are required. The inventoried data is stored in a Microsoft SQL Server database. If you don't have SQL Server, the WVHA setup wizard will prompt you to download and install SQL Server 2005 Express Edition from Microsoft; it'll work just fine. The reports will be created using either Microsoft Office Word 2007 and Microsoft Office Excel 2007 or Word 2003 SP2 and Excel 2003 SP2. (If you don't already have Microsoft Office 2007, you might want to go to http://us20.trymicrosoftoffice.com/default.aspx and download the free 60-day trial version.)

You need a local user account that has administrator privileges for the computers you want to scan and inventory, and the file and printer sharing service (found in your NIC properties) must be enabled. WVHA 2.0 can scan and inventory up to 25,000 computers. The supported desktop OSs WVHA can scan are Vista, XP SP2, and Windows 2000 Professional. The supported server OSs are Windows Server 2003 R2, Windows 2003, and Windows 2000 Server.

To install WVHA, select it in the Downloaded section of the Components pane and click the Browse button to display the setup program. Double-clicking the setup program launches the WVHA setup wizard. Choose where you want to install WVHA, and you're finished.

Running WVHA

Open WVHA and launch its wizard by clicking Start, All Programs, Windows Vista Hardware Assessment. The wizard prompts you for a SQL Server database in which to store the inventory data. You can either create a new database, as shown in Figure 2, page 64, or use an existing one. If you'd like to add the information to an existing database, select *Use an existing database.* Click Next. The wizard then lets you choose to collect information from computers in your environment, generate inventory and assessment reports, or connect to Microsoft.com to download the most current hardware compatibility information.

Next, WVHA needs to find the computers you've chosen to be scanned and inventoried. Find the computers by selecting from among the following options on the Computer Discovery page:

- The *Use the Windows networking protocols* option uses the Computer Browser service to retrieve a

Learning Path

WINDOWS IT PRO RESOURCES

"How Does Vista Rank Among the Past Year's Microsoft Releases?" InstantDoc ID 96088

"Is Vista IT-Ready?" InstantDoc ID 95205

MICROSOFT RESOURCES

"BDD 2007 Demo"
http://www.microsoft.com/technet/desktopdeployment/demos/index.html

"Microsoft Solution Accelerator for Business Desktop Deployment 2007"
http://technet.microsoft.com/en-us/library/bb490308.aspx

"Windows Vista Team Blog: Announcing the release of BDD 2007 to simplify Windows Vista and Office deployments"
http://windowsvistablog.com/blogs/windowsvista/archive/2007/01/17/announcing-the-final-release-of-bdd-2007-to-simplify-windows-vista-and-office-deployments.aspx

Steps for Preparing for VISTA DEPLOYMENT

Are you considering an upgrade to Vista? Be sure to follow these steps before moving forward with a deployment.

STEP 1 Download and install Microsoft's Solution Accelerator for Business Desktop Deployment 2007. It will make Vista deployment a lot easier.

STEP 2 Create a complete software and hardware inventory of all the computers in your environment.

STEP 3 Analyze the reports that are created to determine which computers are upgradeable to Vista and which are not. You may need to purchase larger hard drives or more RAM.

STEP 4 Test all your applications to ensure that they will run properly in a Vista world.

STEP 5 Document the results of your testing every step of the way. You may need to back up a step or two to get the desired results.

InstantDoc ID 96907

list of known workgroups and domains on the local subnet. If you're in a workgroup environment with more than one subnet or a Windows NT 4.0 domain, you'll need to run WVHA on each subnet.

- The *Use Active Directory Domain Services* option sends an LDAP query to a domain controller to retrieve a list of computer objects from Active Directory (AD).
- The *Import computer names from a file* option lets you create a text file containing the names of the computers that you want to scan.
- The *Manually enter computer names and credentials* option lets you manually enter the name of each computer that you want WVHA to scan and the credentials for a local administrator account for that computer.

For testing purposes, or if I have only a few computers to scan, I use the third or fourth option.

The options you choose on the Computer Discovery page determine the subsequent pages you see. For example, when you select the Windows networking protocols option, the next page is the Windows Networking Protocols page. Your workgroups and domains should be listed on this page. If the list is empty, ensure that the Computer Browser service is running on the computer on which you're running WVHA.

When you choose Active Directory Domain Services, the Active Directory Inventory page is displayed and lets you specify the DNS domain name and credentials for an account that has read access to retrieve a list of AD objects. Usernames and passwords entered in the WVHA tool are not stored locally; they're encrypted and stored in RAM, so you need to re-enter the credentials every time you run WVHA.

After you authenticate to AD, the Active Directory Inventory Options page appears. On this page you can choose to find all computers in all domains or specific computers from a particular domain, organizational unit (OU), or container.

To scan for software and hardware inventory, WVHA needs an account that has local administrator privileges on all computers. You can specify as many accounts as you need on the Inventory Accounts page. You can specify one administrative account for all the computers in a specific domain or OU, or you can manually type each computer name with a different set of local administrative credentials.

The Summary of Actions to be Performed page lists the selections you've configured in the wizard. Before you click Start to begin the scan, be sure the machines you want to scan are connected to the network and powered on. When the scan completes, the Your Report is Ready page is displayed. From this page you can choose to rerun WVHA, open the reports folder (more on reports later), or view a detailed summary of the wizard's operation. The summary of wizard operations is great for troubleshooting purposes; each step of the WVHA process generates a completion code that indicates whether the process succeeded or failed.

The WVHA Reports

WVHA generates a full report and a summary and stores them in the My Documents\WVHA\Reports*database name* folder of the user who

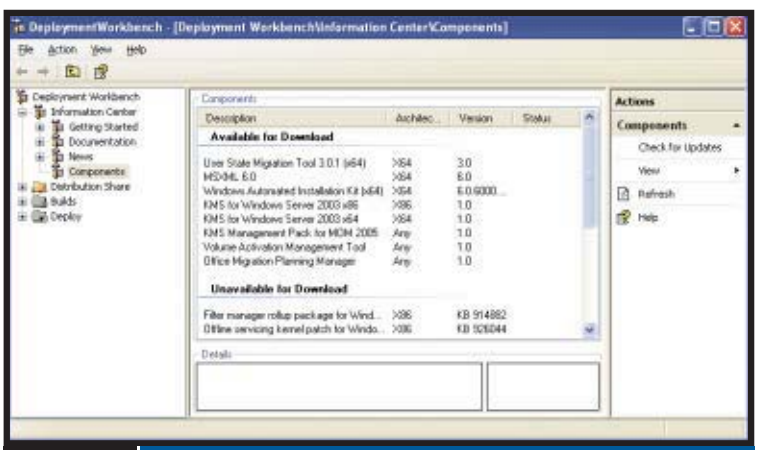


Figure 1: Deployment Workbench

Figure 2: Specifying a database

ran WVHA. For example, if I do an inventory and store it in database named VHA, the reports are stored in My Documents\WVHA\Reports\VHA. The report names also inherit the name of the database—for example, VHA Report 20070704 110402.xlsx and VHA Summary 20070704 110410.docx.

The full report in the Excel workbook contains many worksheets and was designed for systems administrators. The information you'll see in this report includes WMI status (running or not), IP information, service pack levels, hardware and software inventory, the current version of Office and whether it can be upgraded to Office 2007, and whether the computer is upgradeable to Vista. If it isn't, you'll see a list of tasks to perform in order to make it upgradeable.

The summary report is a Word document designed for management. The management report comes complete with beautiful pie charts and tables identifying the number of computers that are capable of upgrading to Vista, as well as the number that are not upgradeable and why. Although the reports contain a plethora of information, you won't find information on whether your computers are capable of running BitLocker Drive Encryption or Aero Glass.

WVUA

To open the WVUA, click Start, All Programs, Windows Vista Upgrade Advisor. Click Start Scan, and you're off. The WVUA takes a few minutes to run, so be patient. Once the scan is complete you'll see a high-level report.

In Figure 3, the Upgrade Advisor suggested installing Vista Home Premium on the XP machine I ran it on. Notice at the bottom of the report there is a yellow yield sign under System Requirements. Click the See Details button to get more information, and you'll see a report like the one in Figure 4, page 66.

Notice that there are four tabs on this report: System, Devices, Programs, and Task List. In the System tab I found that I needed to free up more hard drive space—in order to upgrade I needed at least 15GB free. The Devices tab listed several devices that WVUA couldn't find information for (such as my VMware NIC—go figure) as well as devices for which WVUA found no problems. I really like the feature that scanned all installed printer drivers for Vista compatibility even though only one printer was connected when I ran WVUA. The Programs tab listed several applications that might have problems after I upgrade to Vista, such as Windows Messenger, some older versions of Adobe software, and WinZip. If you have an application that should be upgraded to the most current version, now is the time to do it.

The Task List tab combines information from all the other tabs to provide a to-do list for before and after the upgrade to Vista. You can choose to print the task list or save the report from the top right corner of the page.

ACT 5.0

The ACT helps you determine which applications will run properly in an upgrade and which might encounter problems. Microsoft has created an ACT community where companies report known upgrade-related problems and fixes (called "mitigations") for applications. To learn more about this community, see http://technet2.microsoft.com/WindowsVista/en/library/3f5669fd-6b8f-4b27-a49c-1e865d8f064e1033.mspx.

Figure 3: Sample WVUA report

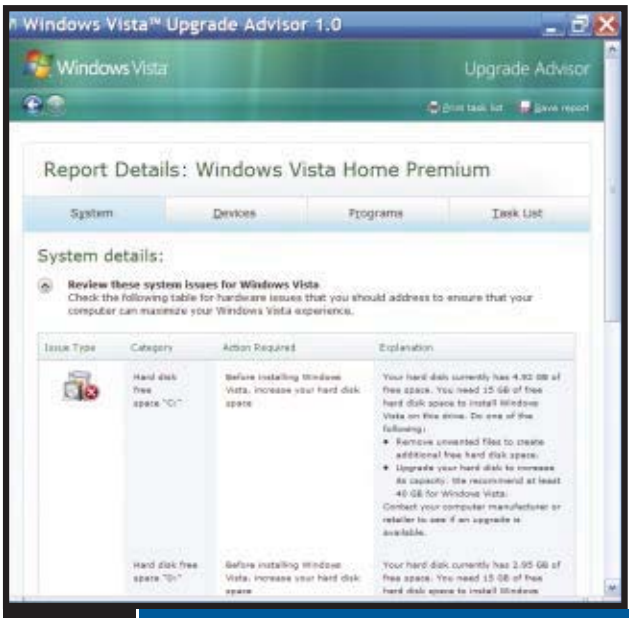


Figure 4: WVUA report details

To install ACT from within BDD, select Application Compatibility Toolkit from the list of downloaded components and click the Browse button in the Detail pane. Then double-click Application Compatibility Toolkit.msi. When the setup wizard is launched, choose the folder in which you want to install ACT, and you're finished.

There are four steps to running ACT: configuration, creating a collection package, deploying the package, and analyzing the data. Before you configure ACT, create and share a folder in which to log the inventory data. Open Application Compatibility Manager (ACM) from Start, All Programs, Microsoft Application Compatibility Toolkit 5.0. The ACT configuration wizard runs the first time you launch ACM. There are two modes: Enterprise mode and View and Manage Reports Only mode. Choose Enterprise mode to create, view, and manage ACT projects and reports. Next, choose your SQL Server or SQL Server Express database. Select the shared folder you created earlier in which to log the inventory data. All computers that will log inventory data need read/write access to the shared folder. Finally, supply a user account and password that will collect that log information in the database. If you choose a specific account, that account must have *Log on as a service* user rights and read/write access to the shared log folder you created and to the database. If you need to edit these configuration settings later, just select Settings from the Tools menu within ACM.

Create a data collection package from ACM's Collect pane by selecting New from the File menu. Give the package a name, choose the compatibility option, and specify when the monitoring should begin and in which database ACM should store the collected information. To select the type of information to be collected, click Advanced and choose the compatibility evaluators (i.e., agents) you want to deploy. There are compatibility evaluators for collecting information on inventory, Microsoft Internet Explorer (IE), User Account Control compatibility, updates (evaluates Windows updates), and Vista (determines if that computer is upgradeable or not).

After you've selected your compatibility evaluators, choose Save and Create Package from the File menu. A self-extracting .exe is created that you can deploy via Group Policy, email, CD-ROM, or a network share. When the collection package is deployed, the compatibility evaluators are installed locally on each computer. The compatibility evaluators run based on the schedule you've set in your collection package.

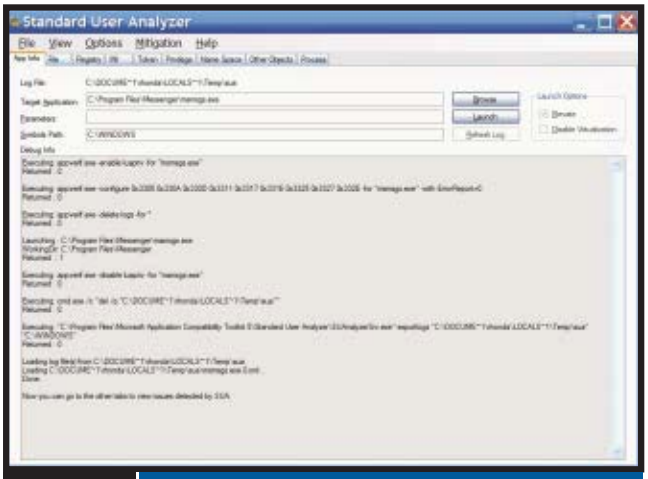


Figure 5: Sample SUA analysis

The last step is to analyze the data that has been collected. Reports identify Vista, XP, IE 7, and Windows Update upgradeability. You can then use the ACT community to view assessments from other companies or create your own assessments.

Developer and Tester Tools

The tools designed for developers to test their applications are the Internet Explorer Compatibility Test (IECT) tool, the Setup Analysis Tool, and the Standard User Analyzer (SUA) tool. These tools are found at Start, All Programs, Microsoft Application Compatibility Toolkit 5.0, Developer and Tester Tools.

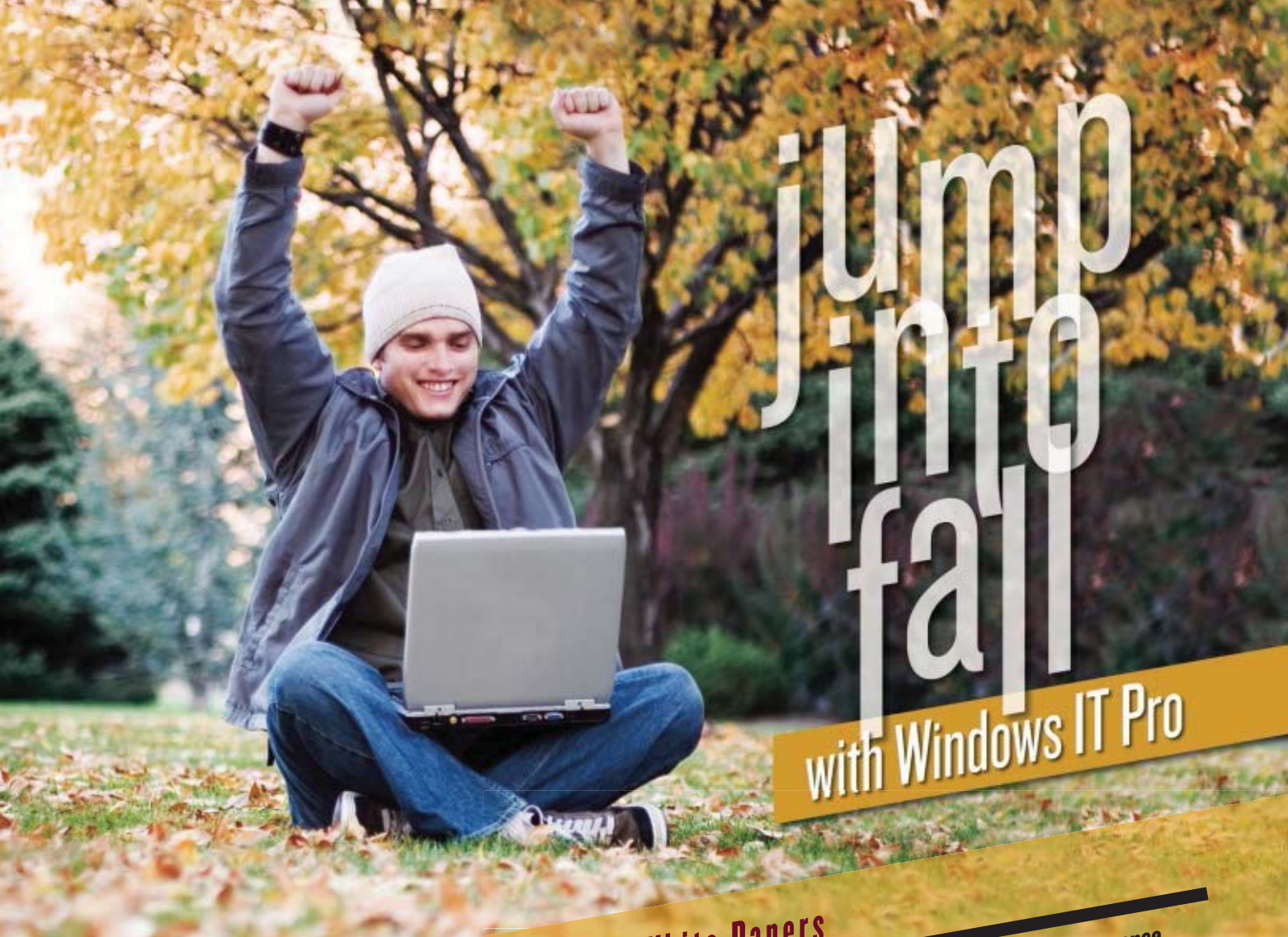
The IECT identifies potential problems with existing Web sites or Web-based applications before you upgrade them to IE 7. Start IECT and choose Logging Enabled from the Tools menu. Now, open IE and browse to a Web site or launch a Web-based application. In IECT under Issue Description (at the bottom of the screen) is a list of possible problems you can address before upgrading.

The SUA tool monitors the installation of an application and reports problems that need to be addressed before the application will run properly on Vista. Once you have a list of problems, you can apply fixes. These fixes are called "mitigations." Mitigations allow you to resolve some of the issues. SUA requires Microsoft's Application Verifier 3.3 (which is a separate download from Microsoft). Once you've downloaded and installed Application Verifier, open SUA, browse to an application's .exe file, then click the Launch button.

As you can see in Figure 5, there are nine tabs that display information showing you exactly what changed, files that were added or edited, registry keys that were added, and so forth. The App Info tab records the steps of the installer program. Changes that the application made to files, the registry, or .ini files are recorded in the File, Registry, and INI tab, respectively. Using the Privilege tab to find privilege levels can be a huge help.

This completes our quick trip through Microsoft's planning tools. They will make your life much easier by helping you identify and resolve Vista upgrade problems.

InstantDoc ID 96906



jump into fall

with Windows IT Pro

Choose from 38 white papers, 37 eBooks, 22 podcasts, and 61 web seminars to get a jump ahead this Fall.

A multitude of information is just a click away at

www.windowsitpro.com

Windows IT Pro

Featured White Papers

KVM over IP Management in the "Distributed IT" Environment

Keyboard/video/mouse (KVM) switches are a valuable server management tool. This paper presents the complexities of managing the distributed data center and highlights the advantages of using a KVM over IP solution that delivers flexible, scalable and affordable CAT5-based remote access.

www.windowsitpro.com/go/lantonix/octad

How Websense Technology Protects Against Internet-Based Threats

The Internet—with its wealth of information and features that have become integrated into our everyday lives—has become a necessary tool for business and also provides a vast array of options for personal use. However, it does have a dark side. This white paper will examine technologies that will help guard against Internet-based threats.

www.windowsitpro.com/go/websense/octad

Automating System Performance and Reliability

File fragmentation is a serious problem. As a disk gets more fragmented the workload on the operating system and hardware increases. It becomes more difficult for applications to read and write data, file corruption becomes a distinct possibility, the user experience is negatively affected due to system performance issues, and the reliability of the computer is endangered. In this white paper we will look at the impact of disk defragmentation on your users.

www.windowsitpro.com/go/diskeeper/octad

Enterprise Messaging Management for Microsoft Exchange

Learn how Symantec and IBM deliver a comprehensive archiving solution to capture and store email, files, instant messaging, databases, VoIP as well as many other document formats—while helping to reduce storage costs and simplifying management. Understand the challenges surrounding an Exchange environment and the Symantec and IBM capabilities to solve them.

www.windowsitpro.com/go/symantec/octad

The Best Conference Bet for IT Pros

Over 250 in-depth sessions, 150 Microsoft Architect and industry expert speakers, and exciting announcements!

November 5-8, 2007

LAS VEGAS, NEVADA
Mandalay Bay Resort and Casino

KEYNOTES


SCOTT GUTHRIE


MARK MINASI


STEVE RILEY


TONY REDMOND

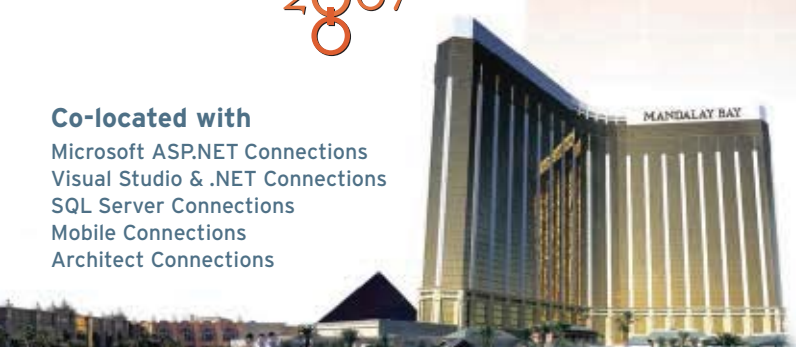
MICROSOFT EXCHANGE Connections 2007

WINDOWS Connections 2007

SharePoint Connections 2007

Office Connections 2007

Co-located with
Microsoft ASP.NET Connections
Visual Studio & .NET Connections
SQL Server Connections
Mobile Connections
Architect Connections



CONNECTIONS RAISES THE BAR FOR IT CONFERENCES, DELIVERING:

- EXPERT SPEAKERS
- UNPARALLELED WORKSHOPS
- DYNAMIC CONTENT
- HOT LOCATION
- EXCITING ANNOUNCEMENTS

REGISTER TODAY!

THIS EVENT SOLD OUT LAST FALL!

WinConnections.com ■ 800-505-1201 ■ 203-268-3204

Every Attendee to Receive: Windows Server 2008 RC1

Microsoft · Windows IT Pro · TechNet Magazine · Tech Conferences Inc. · Penton Media

Office & SharePoint PRO

officeandsharepointpro.com

Introducing the Business Data Catalog

Exploit key business data via MOSS 2007

by Kevin Laahs

Microsoft Office SharePoint Server (MOSS) 2007 provides a service called the Business Data Catalog (BDC). The primary purpose of the BDC is to unlock and expose data held in back-end line of business (LOB) applications so that people, processes, and other information can easily and seamlessly link to that data. As long as someone (typically a developer) has a solid understanding of the data, the BDC can make that data pervasive throughout the MOSS platform. In this article I look at the architecture of the BDC and, by way of an example, reveal its power.

The Business Data Catalog

As its name suggests, the BDC is a catalog of business data. As such, it doesn't physically store business data. Think of a shopping catalog that you've recently viewed. What does it contain? That's right—*descriptions* of items that you can then physically go retrieve. So the BDC is a metadata-driven connector that describes the data, describes how to connect and retrieve that data, and physically retrieves the data on request. The data remains in the back-end application, with the BDC acting as a read-only conduit to it. It will cache some data and some data is physically copied into SharePoint but you need to find another vehicle if you want to write to the back-end data.

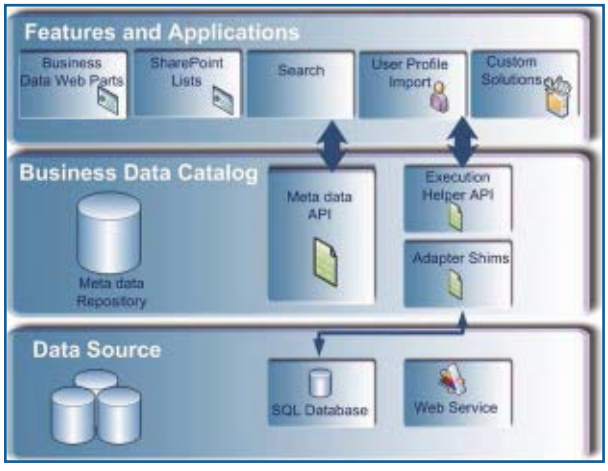


Figure 1: *The BDC architecture*

You can use multiple vehicles to access the data described in the BDC. Out-of-the-box, MOSS lets you access the data through Web Parts, columns in lists and libraries, fields in user profiles, and via search results. And, of course, if you do want to write some code, you can harness the BDC for custom purposes as well. But, as we will see, you can do very powerful things without lifting one coding finger. Figure 1 shows the logical architecture of the BDC.

Describing Data: The Application Definition File

I make it sound so simple by saying you don't need to write any code, don't I? Although this is true, you do need to do some groundwork to describe the data, and this will take effort on the part of the business application owner and someone from IT who's knowledgeable about the physical storage of the data and possible access methods. The application owner will describe the purpose of the data and how it's linked to meet a particular business requirement. The IT person will then create an application definition file (ADF), an XML file

Learning Path

WINDOWS IT PRO RESOURCES

Learn about SharePoint:

"SharePoint Server 2007 Revealed," InstantDoc ID 94914

"SharePoint Security Evolution," InstantDoc ID 94335

MICROSOFT RESOURCES

Business Data Catalog: Overview
http://msdn2.microsoft.com/en-us/library/ms551230.aspx

Application Definition File Reference
http://msdn2.microsoft.com/en-us/library/aa225517(SQL.80).aspx

Welcome to the Microsoft Office SharePoint Server 2007 SDK
http://msdn2.microsoft.com/en-us/library/ms550992.aspx

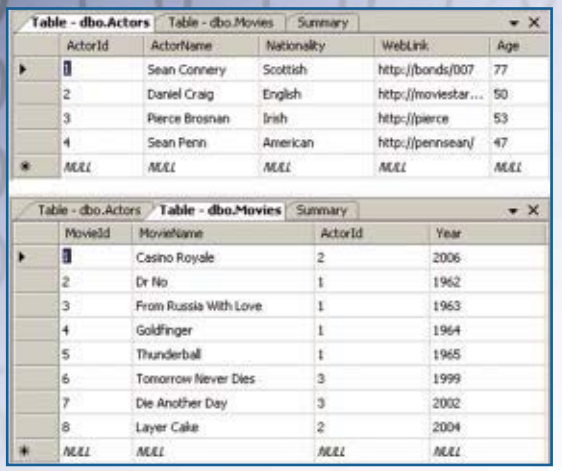


Table - dbo.Actors | Table - dbo.Movies | Summary

ActorId	ActorName	Nationality	WebLink	Age
1	Sean Connery	Scottish	http://bonds/007	77
2	Daniel Craig	English	http://moviestar...	50
3	Pierce Brosnan	Irish	http://pierce	53
4	Sean Penn	American	http://pennsean/	47
NULL	NULL	NULL	NULL	NULL

Table - dbo.Actors | Table - dbo.Movies | Summary

MovieId	MovieName	ActorId	Year
1	Casino Royale	2	2006
2	Dr No	1	1962
3	From Russia With Love	1	1963
4	GoldFinger	1	1964
5	Thunderball	1	1965
6	Tomorrow Never Dies	3	1999
7	Die Another Day	3	2002
8	Layer Cake	2	2004
NULL	NULL	NULL	NULL

Figure 2: *Sample data to expose using BDC*

that describes the data, and load the file into the BDC.

The BDC supports two data access methods—direct calls to most popular databases via ADO.NET, OLE DB, and ODBC drivers or calls to application-specific Web services that can gather and return the desired data. Because of space limitations, I'll tackle the Web services method at a later time. In this article, I use a simple database example that will expose the data shown in the two tables that Figure 2 shows, with the end result being a page shown in a standard MOSS team site, as Figure 3 shows. The business purpose of these tables is to list all the movies an actor has appeared in. An analysis of the data shows that the ActorId column links the two tables for such a purpose, with the Actor table being the parent table and the Movie table being the child.

Forget the BDC for a second and imagine the main coding stages you'd need to go through to achieve such a result. First, you'd need to identify and connect to the database with suitable credentials. Next you'd need to open the tables and run some queries that return various rows and columns (e.g., one to gather the parent item and one to link the parent to its child items). So you'd need to define the relationship between the parent and child and the columns that you want returned. Finally, you'd need to format and display the returned data.

The BDC removes the complexity of this process, and the ADF essentially describes how to perform each of these stages except data formatting and display. That step is performed by BDC-aware Web Parts, list columns, user profile properties, and search.

The ADF must be well-formed and adhere to the schema defined at C:\Program Files\Microsoft Office Servers\12.0\Bin\bdcmetadata.xsd on a SharePoint Web front-end server. The schema defines connections, entities, methods, filters, actions, and relationships. Let's look at each of these components and the associated XML code that I used to deliver our example. You can download the entire XML metadata file from *Windows IT Pro*'s Web site. (Go to http://www.windowsitpro.com, enter 96772 in the InstantDoc ID text box, then click *Download the Code*.)

Connections

The LOBSystemInstance node in Listing 1, page 72, defines authentication and connection information such as which database instance to connect to and which catalog to open. (Note that some lines wrap because of space limitations.) From an authentication point of view, the BDC can access the database as a system account or as the calling user.

The code shows that I've defined an instance called SpiesInstance. It accesses a table called Spies in a SQL Server database called dc2\sqlexpress using the credentials of the calling user. The calling user therefore will need permissions to access the data.

Figure 3: *Sample data shown in MOSS 2007 team site*

Entities

An entity describes an item in the LOB application. The code in Listing 2, page 72, defines two items: an actor and a movie. Each entity contains child nodes that define identifiers, methods, filters, and actions. Think of the identifier as the primary key within a database table. It uniquely identifies a particular instance of an entity, which, in our case, are the primary keys called ActorId and MovieId. (Note some sound advice from a badly scarred human being: The XML is case-sensitive so make sure the names match the database columns.)

The properties node defines some characteristics of the entity. The code in Listing 2 shows that the ActorName and MovieName columns will be the default display value that's returned for the entity. It also associates a default action called View Profile that I discuss later.

Methods

The methods component defines the methods by which you can locate instances of an entity, much like an interface definition. For example, a method can be a SQL statement, a stored procedure for a database, or a Web method for a Web service. Certain methods must be defined for certain SharePoint functionality to function. For example, you must define an IDEnumerator method if the data is to be indexed by the search engine. This method returns all the valid Entity IDs so that it can crawl through all instances of the entity. The MOSS 2007 software development kit (SDK), available at http://msdn2.microsoft.com/en-us/library/ms550992.aspx, provides more details about methods instance types and how to use them for different types of SharePoint functionality.

Listing 3, page 72, shows that for the Actor entity, I've defined two methods: GetActors and GetMoviesForActor. Both of these run appropriate SQL statements to return the desired result based on some input parameters. For each entity you must define a method instance that will return one instance of that entity (type=SpecificFinder) and a method instance to return multiple instances of that entity (type=Finder). Failure to do so will result in errors when you use a Web Part, list, or search to consume the data. In this example, I use the GetActors method to return one or all of the actors.

Parameters

You need to define input parameters that will be used as filters to queries at the backend. Some default Web Parts let you choose which input

parameters to filter on. You also need to define the return parameters for each method. You can see in Listing 4, page 73, that I defined a filter called Name that will perform a wildcard comparison. I then associated that filter with the input parameter that relates to the ActorName column (see the AssociatedFilter attribute of the TypeDescriptor node that describes the Actor Name input parameter).

Listing 2 also shows a parameter whose name attribute is Actors. This is where I describe which columns from the table I want returned and what display names to use for them.

Listing 1: Defining Connections

```
<LobSystemInstances>
  <LobSystemInstance Name="SpiesInstance">
        <Properties>
                <Property Name="AuthenticationMode"
                  Type="Microsoft.Office.Server.ApplicationRegistry.
                  SystemSpecific.
                  Db.DbAuthenticationMode">PassThrough</Property>
                <Property Name="DatabaseAccessProvider"
                  Type="Microsoft.Office.Server.ApplicationRegistry.System
                  Specific.Db.DbAccessProvider">SqlServer</Property>
                <Property Name="RdbConnection Data Source"
                  Type="System.String">dc2\sqlexpress</Property>
                <Property Name="RdbConnection Initial Catalog"
                  Type="System.String">Spies</Property>
                <Property Name="RdbConnection Integrated Security"
                  Type="System.String">SSPI</Property>
        </Properties>
  </LobSystemInstance>
</LobSystemInstances>
```

Actions

Actions are independent operations that can apply to an entity. You describe them in the BDC, and they're surfaced in the relevant places. For example, defined actions will appear in the Actions menu of the Business Data List Web Part. You can use them to do almost anything—such as, provide a quick link to the source data through the source application for full access to the data or link to any location based on the returned data. For example, you might want to link to a Google or Windows Live search and pass a piece of returned data into the search.

View Profile is a default action that you get with every entity. You can see in Web Listing 1 (which you can view at http://www.windowsitpro.com, InstantDoc ID 96772) that I added two other actions. One will feed the actor's name into a search on the Internet Movie Database, and the other will launch the URL that's associated with the WebLink column in the actor's entry in the Actors table. You can also add more actions through SharePoint after the entity is defined within the BDC.

Listing 2: Defining Entities

```
<Entity EstimatedInstanceCount="100" Name="Movie">
  <Properties>
        <Property Name="Title" Type="System.String">MovieName</Property>
        <Property Name="DefaultAction" Type="System.String">View Profile</Property>
  </Properties>
  <Identifiers>
        <Identifier Name="MovieId" TypeName="System.Int32" />
  </Identifiers>
  <Methods>
  <Actions>
  </Entity>
<Entity EstimatedInstanceCount="100" Name="Actor">
  <Properties>
        <Property Name="Title" Type="System.String">ActorName</Property>
        <Property Name="DefaultAction" Type="System.String">View Profile</Property>
  </Properties>
  <Identifiers>
        <Identifier Name="ActorId" TypeName="System.Int32" />
  </Identifiers>
  <Methods>
  <Actions>
  </Entity>
```

Listing 3: Defining Methods

```
<Method Name="GetActors">
  <Properties>
        <Property Name="RdbCommandText" Type="System.String">SELECT * FROM
          dbo.Actors WHERE (ActorId >= @MinActorID) AND (ActorId <= @MaxActorId)
          And (ActorName LIKE @ActorName)</Property>
        <Property Name="RdbCommandType"
          Type="System.Data.CommandType">Text</Property>
  </Properties>
  <FilterDescriptors>
  <Parameters>
  <MethodInstances>
        <MethodInstance Name="ActorFinderInstance" Type="Finder"
          ReturnParameterName="Actors" />
        <MethodInstance Name="ActorSpecificFinderInstance" Type="SpecificFinder"
          ReturnParameterName="Actors" />
  </MethodInstances>
</Method>
<Method Name="GetMoviesForActor">
  <Properties>
        <Property Name="RdbCommandText" Type="System.String">Select MovieId,
        MovieName, Year From Movies Where ActorId=@ActorId</Property>
        <Property Name="RdbCommandType" Type="System.String">Text</Property>
  </Properties>
  <Parameters>
</Method>
```

Associations

Associations link entities together. A typical example would be two tables in a database that have a one-to-many relationship. In our example, I use a relationship to link an actor to the movies he or she appears in, as Web Listing 2 shows. The association defines the name of the method to use to form such a relationship.

As you can see, defining the contents of the ADF requires knowledge about the implementation of the back-end application. Creating the correct XML is never a trivial task, but you can find XML samples that use the AdventureWorks2000 SQL Server sample database in the MOSS SDK. There are also some community tools and third-party applications—such as http://www.bdcmetaman.com/default.aspx—starting to appear that can help generate the right ADF for the job at hand.

Importing an ADF

After you define the ADF, you have to import it into the Shared Services Provider; the BDC is a shared service and as such can be used by any Web Application or site that's associated with that shared service. You do this from the Shared

JOIN US THIS FALL IN LAS VEGAS AT THE CUTTING-EDGE EVENT FOR IT PROFESSIONALS!

Over 240 in-depth sessions from Microsoft and industry experts, 150 speakers, and exciting announcements!

CONNECTIONS RAISES THE BAR FOR IT CONFERENCES, DELIVERING:

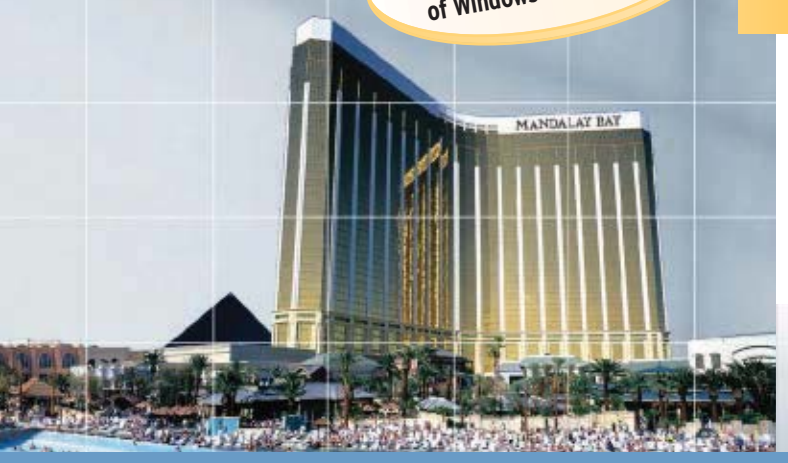
- Expert Speakers
- Unparalleled Workshops
- Hot Location
- The most relevant, up-to-date content on the eve of Visual Studio 2008 and Windows Server 2008

NOVEMBER 5-8, 2007

LAS VEGAS, NEVADA
Mandalay Bay Resort and Casino

Co-located with
Microsoft ASP.NET Connections
Visual Studio & .NET Connections
Architect Connections
SQL Server Magazine Connections
Mobile Connections
OpenForce 07′

EVERY ATTENDEE TO RECEIVE the latest pre-release version of Windows Server 2008



MICROSOFT EXCHANGE Connections 2007

WINDOWS Connections 2007

SharePoint Connections 2007

Office Connections 2007

REGISTER TODAY!

WinConnections.com ■ 800-505-1201 ■ 203-268-3204

Microsoft® Windows IT Pro MAGAZINE TechNet MAGAZINE TECH Conferences LLC PENTON MEDIA

Join us
IN LAS VEGAS FOR CONNECTIONS 2007

IMMERSIVE EDUCATION FROM MICROSOFT AND THE WORLD'S TECHNOLOGY EXPERTS

- Choose from over 240 in-depth, no-hype sessions delivered by Microsoft and industry experts
- Get the scoop from Microsoft and independent, world-renowned experts in one event: the most well-rounded perspective of any technology event
- The best blend of sessions: where novice means novice and advanced means advanced
- Unique, hands-on Exchange troubleshooting, PowerShell, and virtualization workshops
- Learn the tips and tricks it takes to make the technology work based on real-world experience, not product marketing hype
- Dive into our highly focused pre- and post-conference workshops on Exchange, SharePoint, deployment, virtualization, security, Group Policy, and advanced Windows administration
- Explore the partner exposition, pick up great giveaways, and enter the contest to get the chance to drive home on a Harley-Davidson motorcycle
- Gain insights from hundreds of other participants who represent *experienced* IT professionals from a wide range of industries and enterprises
- Unwind and network with your peers at Mandalay Bay Resort and Casino.

TABLE OF CONTENTS

SCHEDULE AT A GLANCE

SUNDAY, NOVEMBER 4, 2007

8:00 am - 11:00 am	Pre-conference Workshop Registration ONLY
9:00 am - 4:00 pm	Pre-conference Workshops

MONDAY, NOVEMBER 5, 2007

7:00 am - 5:00 pm	Conference Registration
9:00 am - 4:00 pm	Pre-conference Workshops
6:30 pm - 8:30 pm	Microsoft Executive Keynote
8:30 pm - 10:30 pm	Expo Hall/Dessert Reception

TUESDAY, NOVEMBER 6, 2007 • MICROSOFT DAY

7:00 am - 5:00 pm	Conference Registration
7:00 am - 8:00 am	Continental Breakfast
8:00 am - 9:00 am	Keynote
9:30 am - 10:30 am	Conference Sessions
10:45 am - 11:45 am	Conference Sessions
11:45 am - 1:30 pm	Lunch
1:30 pm - 2:30 pm	Conference Sessions
2:45 pm - 3:45 pm	Conference Sessions
4:15 pm - 5:15 pm	Conference Sessions
5:15 pm - 6:30 pm	T-Shirt/Software Giveaway

WEDNESDAY, NOVEMBER 7, 2007

7:00 am - 5:00 pm	Conference Registration
7:00 am - 8:00 am	Continental Breakfast
8:00 am - 9:15 am	Conference Sessions
10:00 am - 11:15 am	Conference Sessions
11:30 am - 12:45 pm	Conference Sessions
12:45 pm - 2:15 pm	Lunch
2:00 pm 2:15 pm	*Harley-Davidson Drawing in the Expo Hall* Expo Hall Closes
2:15 pm - 3:30 pm	Conference Sessions
4:15 pm - 5:30 pm	Conference Sessions

THURSDAY, NOVEMBER 8, 2007

7:00 am - 8:00 am	Continental Breakfast
8:00 am - 9:15 am	Conference Sessions
9:30 am - 10:45 am	Conference Sessions
11:30 am - 12:30 pm	Conference Sessions
12:30 pm - 2:00 pm	Lunch
2:00 pm - 3:00 pm	Conference Sessions
3:00 pm - 3:30 pm	Ice Cream Break
3:30 pm - 4:15 pm	Closing Session

FRIDAY, NOVEMBER 9, 2007

9:00 am - 4:00 pm	Post-conference Workshops

SEE WEB SITE FOR THE LATEST SCHEDULE UPDATES.
www.WinConnections.com

Exciting Microsoft Executive Keynote to be announced!

(Check Web site Aug 1 for more details)

MAKING THE TRADEOFF: BE SECURE OR GET WORK DONE

STEVE RILEY MICROSOFT

Are you the kind of security person who enables a setting just because it's there? Do your users constantly seek ways to bypass all your fine-tuned security, just so they can do their jobs? Every security decision your organization makes ought to consider the security-usability (or even the security-usability-cost) tradeoff. While perfect security seems an admirable goal, in reality we must remember that usability often will trump our strongest desires. If people can't get work done, they'll either circumvent the security (without understanding they just created new attack vectors) or your company will simply lose out to your competitors. Steve Riley will discuss several examples of real-world tradeoffs and will help you learn how to navigate the tradeoff in your own organization.

LIVING THE LONGHORN LIFE: WHAT'S UP WITH WINDOWS SERVER 2008

MARK MINASI MR&D

Microsoft released the new desktop, Windows Vista, in November 2006... but that's just the start. A new version of Server's right on its heels—formerly code-named "Longhorn Server," it'll be named Windows Server 2008, and it will pack a ton of new stuff, from some really good news in Active Directory to some nifty new deployment tools, a quarantine system that'll help you keep the worm-ridden systems off of your network, a revamped Web server, and a few truly long-awaited changes in group policy. How can you find out about all of this? Well, you could download a few terabytes worth of white papers and start sifting through them to separate the wheat from the chaff, or you could attend this short session by Mark Minasi, the guy who's been explaining new operating systems since Windows 1.0. Come to this session and find out why Server Core may be your favorite new piece of software!

NEXT GENERATION MESSAGING

TONY REDMOND HP

Microsoft Exchange 2007 is very different to the generations of Exchange that have gone before and forces administrators to consider new ways of deploying the Exchange ecosystem onto a Windows 64-bit platform. All we can guarantee about technology is that change will continue to occur or even accelerate as new hardware and software technologies influence the design decisions that groups like the Exchange engineering team make as they work on new versions of Exchange to appear in the 2010-2015 timeframe. This session discusses some of the technology directions that may influence the way that Exchange evolves, including virtualization, mobility, information lifecycle management, unified communications, automation, and software as a service.

THE FUNGIBLE FUTURE: THE CREATION OF COOL AND CONSUMERIZATION OF I.T.: A PANEL DISCUSSION

ROMI MAHAJAN MICROSOFT

As the pace of change increases in the world of information technology, job-roles, personas, affinities, and alliances change just as rapidly. Ultimately, lines of distinction blur between the roles of IT professionals and developers, between "work-related" technologies and "consumer" technologies, between work-time, play-time, and home-time. In addition, there is a strong relationship and even a causal link between what we think is cool and what we ultimately buy at home with what we think is relevant and what we ultimately buy to run our enterprises. As these lines blur, we find that we are in a world in which the old distinctions melt: the fungible future is upon us now! Please join a renowned panel discussing these trends and helping us all determine what are the next big trends that disrupt and the next steps in the creation of cool.

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE. SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.

EXCHANGE SESSIONS
PRESENTED BY MICROSOFT

MICROSOFT EXCHANGE Connections 2007

It's the all-new, re-architected, more powerful messaging and groupware platform from Microsoft: **Exchange Server 2007!** Packed with new features, new architectural options, and new capabilities, Exchange Server 2007 is also the first fully automatable and command-line-managed server product from Microsoft, leveraging the Windows PowerShell shell and scripting environment. Rely on Exchange Connections to connect you with the most respected and relied-upon subject-matter experts in the world for Exchange Server 2007. **Come to Exchange Connections to:**

- Learn about new architecture options in Exchange Server 2007, including ways of scaling out your Exchange Server environment bigger and better than ever before.
- Discover how Exchange Server 2007 works under-the-hood, including data management, engine details, troubleshooting and disaster recovery, and much more.
- Provide your users with anywhere e-mail access through an all-new Outlook Web Access, mobile e-mail access, and much more.
- Keep your Exchange Server 2007 environment secure with information on internal security, antivirus, anti-spam, and other measures that keep your environment and your users safer.
- Learn about deployment and migration techniques and issues, making your Exchange Server 2007 migration and deployment easier, safer, and faster.

EXCHANGE CONNECTIONS COVERS THE TECHNOLOGIES YOU NEED:

DISASTER RECOVERY
- Continuous Backup
- Standby Cluster Recovery
- Online Backup Recovery

SECURITY
- Sender ID
- Creating and Testing Mail Hygiene

TROUBLESHOOTING
- Troubleshooting Message Flow
- Troubleshooting DNS
- Advanced SMTP Troubleshooting

MIGRATION AND DEPLOYMENT
- Migration Issues
- Deployment Techniques
- Performance Optimization

END-USER FEATURES
- Client Access Server
- Small Business Mobility
- Getting Rid of PSTs

MICROSOFT SYSTEM CENTER DATA PROTECTION MANAGER (DPM) 2007: HOW TO PROTECT MICROSOFT EXCHANGE SERVER

Currently in beta, DPM 2007 is designed to provide a best-of-breed protection and the most robust, reliable recovery experience for Exchange Server, SQL Server, and SharePoint. This session focuses on the specifics of how DPM protects Exchange, including 2003 servers and 2007 CCR and LCR clusters. The session covers specifically how Exchange storage groups and mailboxes are protected and what functionality is available for restore. Be the first to see how DPM 2007 beta 2 protects Exchange and other Microsoft server platforms.

EARLY LOOK AT EXCHANGE 2007 SP1

Interested in learning about the new features and capabilities available in Exchange Server 2007 SP1? This session takes a look at the continued investments made in Outlook Web Access, increased availability models, and new management tasks such as Public Folder administration built into the Exchange Management Console.

GETTING STARTED WITH MICROSOFT EXCHANGE SERVER 2007: SIMPLE INSTALLATION, SETUP, AND ADMINISTRATION SCENARIOS

Exchange Server 2007 is now built on standard Microsoft installer so that you can take advantage of patching services such as the Software Update Service (SUS). This includes new server roles for flexible deployment of the topologies you require and the power to automate installation. These are just some of the new advancements in the Exchange Server 2007 set-up experience. This is a must-see session for a high-level overview and walkthrough of how you will be deploying Exchange 2007.

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE.
SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.

MICROSOFT EXCHANGE 2007 ARCHITECTURE AND DESIGN AT MICROSOFT

Ever wondered how a large enterprise plans and implements design and architecture of its next generation of messaging system? Join us in this session where engineers from the Microsoft IT messaging team uncover the details on how Exchange 2007 infrastructure was introduced and fully deployed in a 120,000+ mailbox production environment. Topics include: messaging topology design, hardware planning for various Exchange server roles, client access server (CAS) and mobility scenarios, transport architecture, mailbox server and storage designs, backup, restore, and high availability strategies.

MICROSOFT WINDOWS POWERSHELL SCRIPTING FOR MICROSOFT EXCHANGE SERVER 2007

This session covers the new Windows PowerShell-based Exchange cmdline and scripting interface. Learn how to convert your multiple page Visual Basic and COM scripts to mere one-liners in Exchange 2007. This session covers the basics of the management shell, as well as the underlying design and key concepts. Additionally, it goes into more depth on how to build larger scripts that you can use to automate small, medium, as well as enterprise business scenarios.

HIGH AVAILABILITY IN MICROSOFT EXCHANGE SERVER 2007 AND EXCHANGE SERVER 2007 SERVICE PACK 1

E-mail has become mission-critical for the large and the small. Businesses and organizations of all types can no longer afford the extended outages of disasters like failed disks, corrupt databases, failed servers, or power outages. Exchange Server 2007 provides simplified in-the-box HA solutions that make recovery from many disasters barely noticeable to end users. Learn how Local Continuous Replication, Cluster Continuous Replication, Standby Continuous Replication, and Single Copy Clusters provide fast recovery for events that used to be called disasters.

EXCHANGE SESSIONS
PRESENTED BY MICROSOFT

THE PRACTICAL DO'S AND DON'TS IN DISASTER RECOVERY FOR MICROSOFT EXCHANGE SERVER 2007

What do you do when a disaster such as component failure, power outage, operator error, malicious activity, or natural disaster out-strips your Exchange 2007 high availability solution? How do you minimize the impact of the disaster and resume business operations as quickly as possible? This session covers practical techniques you can use to recover from system faults, operational best practices that enable business continuity, and barriers to availability and recovery to watch out for.

MICROSOFT EXCHANGE SERVER 2007: TIPS AND TRICKS

This session focuses on troubleshooting tips and tricks for the most common Exchange Server 2007 symptoms encountered by Microsoft Customer Service and Support. These symptom areas include: mailflow, disaster recovery, and performance. The session touches on the capabilities and use of the Exchange Best Practices Analyzer and Database/Mailflow/Performance troubleshooters. Moreover, the session provides additional tips and tricks beyond the capabilities of those tools.

UNIFIED COMMUNICATIONS

ADDING VOICE TO THE ENTERPRISE: THE NEW CAPABILITIES OF MICROSOFT OFFICE COMMUNICATIONS SERVER 2007 AND OFFICE COMMUNICATOR 2007

Be the first to discover the new capabilities of Office Communications Server 2007 and Office Communicator 2007, which will transform the IM, presence, voice, and conferencing scenarios.

MICROSOFT OFFICE COMMUNICATIONS SERVER 2007: A LOOK AT ITS ARCHITECTURE AND DESIGN

This session provides an overview of Office Communications Server (OCS) capabilities, architecture, and topologies. This includes an overview of all infrastructure investments in the OCS 2007 server release, spanning presence, conferencing, voice, and manageability. Next, it drills into the architectural building blocks of OCS, providing a comprehensive overview. Finally, it describes the typical topologies for OCS in different classes of customer environments, including aspects of scale, external access, and geographical distribution.

ON-PREMISE CONFERENCING: DELIVERING ENTERPRISE-CLASS VOICE, VIDEO, AND WEB CONFERENCING WITH MICROSOFT OFFICE COMMUNICATIONS SERVER 2007

This session describes the conferencing capabilities of Office Communications Server (OCS) 2007, explains the infrastructure needed to deliver conferencing capabilities with OCS, and the best practices to plan and deploy the conferencing capabilities of OCS 2007.

PLANNING AND DEPLOYING MICROSOFT OFFICE COMMUNICATIONS SERVER 2007 AND OFFICE COMMUNICATOR 2007

A new range of deployment configurations of Office Communications Server (OCS) 2007 can now support everything from high availability and scalability requirements, to high availability and simplicity requirements, to the need for economical and simple deployment. This session talks about how you can plan to deploy these configurations for companies from 1000 users to one-million users across one or multiple locations. Learn how to control the OCS 2007 capabilities delivered to an individual user or a set of users and manage Office communicator client versions in your enterprise.

MIGRATING FROM MICROSOFT OFFICE LIVE COMMUNICATIONS SERVER (LCS) 2005 TO OFFICE COMMUNICATIONS SERVER (OCS) 2007

This session provides you with up-to-date information on the tools and guidance you need to move from, and co-exist with LCS 2005 SP1 to OCS 2007 platform. The session covers recommended deployment strategies for servers and clients when migrating from LCS 2005 SP1 to OCS 2007. We'll discuss planning aspects when deploying OCS 2007 to co-exist with LCS 2005 SP1 and transitioning to enhanced presence.

VOICE AND VIDEO IN MICROSOFT OFFICE COMMUNICATION SERVER 2007: INSIGHTS TO QUALITY OF EXPERIENCE AND PLANNING FOR NETWORK BANDWIDTH USAGE

Come to this session to learn about how OCS will deliver the best possible quality of experience without requiring QoS on any network, anytime, anywhere. Learn about the comprehensive approach that combines adaptive end-points measuring the experience for all calls at all times, and an advanced media stack that can correct network and non-network impairments.

EXC16: ADVANCED EXCHANGE PROTECTION USING DATA PROTECTION MANAGER

DEVIN L. GANGER

Backing up and restoring Exchange servers is an essential part of keeping your messaging infrastructure up and running, even when you're running an advanced clustering configuration. Why should you consider using the new version of Microsoft System Center Data Protection Manager ("v2") to protect your Exchange server clusters? Is it any harder than backing up standalone servers? This session covers protecting Exchange 2003 and 2007 servers clustered configurations, including the new Exchange 2007 replication options.

EXC02: BEST PRACTICES FOR EXCHANGE 2007 CLUSTERED MAILBOX SERVER (CMS) DEPLOYMENTS

DARAGH MORRISSEY

This session describes how you can deploy Exchange 2007 in scenarios where high availability is a key requirement. This session covers the following topics:

- Overview of Exchange 2007 Clustered Mailbox Servers
- Overview of CCR
- Deployment requirements
- Deployment best practices
- Managing CMS and CCR with PowerShell
- Monitoring CMS with the Exchange 2007 Management Pack
- Managing your CMS deployment with PowerShell

EXC10: BEYOND THE ETHICAL WALL: USING EXCHANGE 2007 TRANSPORT RULES

CHRIS SCHARFF

Most discussions of the new transport rules begin and end with an example of using the new transport rules interface in Exchange 2007 to implement an ethical wall. This session will explore additional examples where you can use transport rules in a broad cross-section of organizations.

EXC20: CONTINUOUS DATA PROTECTION FOR EXCHANGE

PAUL ROBICHAUX

Exchange makes full use of both conventional and point-in-time backup technologies. However, many administrators want more! This session will explain the underpinnings of continuous backup solutions from Microsoft and third-party vendors for Exchange 2003 and Exchange 2007 so you can choose an appropriate solution for your needs.

EXC06: CRASH COURSE TO EXCHANGE SERVER 2007 CLUSTER CONTINUOUS REPLICATION

JUERGEN HASSLAUER

If you managed to get around deploying Exchange clusters in the past and preferred running Exchange on single servers, now is the right time to reevaluate the pros and cons of clustering Exchange. Attend this session and you will get a fast start to CCR. You will learn the architecture of Windows failover clustering and the things you need to know about a Majority Node Set cluster. I will discuss what you have to consider for a geographically dispersed deployment of CCR and how to manage CCR. You will learn in one session what others have learned the hard way. Additionally, I will provide an outlook to the options Windows Server 2008 will provide.

EXC13: EXCHANGE 2003: BEST PRACTICES DAY BY DAY

JIM MCBEE

What should you be doing on a daily basis to keep your Exchange servers stable and running optimally? Topics in this session include the basic tasks that you should perform on every Exchange 2003 server and events to watch for in the event logs. What can you do to improve your Exchange operations, customize your operations, and tweak Exchange to meet the requirements of your organization? Also covered are some "worst" practices in Exchange management such as "over administering" the Exchange server and common configuration mistakes.

EXC08: EXCHANGE 2007 AND COMPLIANCE

KIERAN MCCORRY

Exchange 2007 allows you to implement various e-mail policies that can help you meet your compliance and records management needs. How does this technology work and what considerations do you need to have to make sure your users take advantage of them? This session will cover the major advancements in this area highlighting how you can make the best use of these technologies.

EXC04: EXCHANGE 2007 DESIGNING FOR UNIFIED MESSAGING

ANTHONY VITNELL

The Exchange 2007 Unified Messaging role has introduced a completely new concept for Exchange Administrators. This role introduces new design criteria such as telephony integration, dial plans, and linguistic issues that you must address. In this deep-dive session I will build on real customer experiences and walk through the Unified Messaging design requirements, explain what happens when the UM server receives a call, and look at deployment architectures. In addition, I will discuss the limitations of the Unified Messaging role and provide strategies to work around these limitations. At the conclusion of this session you will have the knowledge required to design the Unified Messaging role for your organization.

EXC14: EXCHANGE 2007 FOR EXCHANGE 2003 ADMINISTRATORS

JIM MCBEE

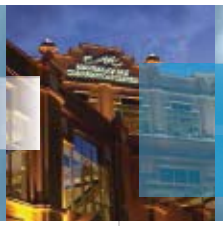
There has been a lot of hype and media attention surrounding Exchange 2007. The Exchange community had their first look at Exchange 2007 in the summer of 2006. But what does the release of Exchange 2007 mean to your users and you as an Exchange 2003 administrator? 64-bit hardware support, a revamped user interface through a new graphical user interface or Monad scripts, continuous replication, resource mailbox support, Edge services, improved mobile support, and unified messaging will all affect the way you manage your Exchange organizations and the services you provide to your user community. Topics in this session will include:

- Determining a migration / upgrade path to Exchange 2007 from your current Exchange environment
- Implementing e-mail lifecycle management
- Implementing Outlook 2007 using the auto-discovery service
- Reviewing the new Exchange server roles
- Using new features for virus protection, spam reduction, and content filtering
- Using the new Exchange Management Console and Monad scriptlets
- Using local continuous replication to improve availability
- Implementing Exchange Edge services
- Reviewing new unified messaging features
- Taking advantage of resource mailboxes and the scheduling assistant

EXC07: EXCHANGE MAILBOX SERVER SIZING

JUERGEN HASSLAUER

Exchange Server 2007 is now a 64-bit application and it removed scalability boundaries of its 32-bit predecessor. No more kernel memory limits and heavily reduced storage performance requirements. Can I now host 10,000 users with 2 GB mailboxes on one mailbox server? Should I give back my expensive SAN array and buy a few cheap large capacity disks for a direct attached storage box? Continuous replication looks great, should I drop the best practice to run daily full backups and put all my faith in the database replica? This session will provide answers to these questions that reappeared during each Exchange Server 2007 migration workshop. This session will also discuss rules of thumb for sizing your Exchange servers and share the findings



from the first production deployments in corporate environments.

EXC17: EXCHANGE MANAGEMENT SHELL ANNOYANCES
DEVIN L. GANGER

The Exchange 2007 Management Shell makes full use of the exciting new Windows PowerShell technology. It's a great command-line management experience, but it's still not perfect. You may have already been tripped up by annoyances and complications in what seem to be obvious tasks or you may just want to know what dangers lurk beneath the surface. This session will show you some common pitfalls and problems and give you the knowledge to successfully navigate them.

EXC18: GETTING RUN OVER BY EXCHANGE 2007
DEVIN L. GANGER

Common knowledge says that upgrading to Exchange 2007 isn't nearly as hard as the upgrade from Exchange 5.5. That's not to say that it doesn't present its own set of challenges—and if you're caught by them, it will still feel like getting run over by a truck. This session will present some of the common gotchas and how to avoid them. Be at the head of the upgrade parade, not caught in the wheels.

EXC01: GETTING THE MOST FROM THE EXCHANGE 2007 MOM MANAGEMENT PACK
DARAGH MORRISSEY

Learn how to deploy the Exchange 2007 Management Pack and leverage the information it provides on the health of your Exchange 2007 deployment. This topic covers the following areas:

- Basics of Microsoft Operations Manager (MOM) 2005
- Overview of the Exchange 2007 Management Pack
- Best practices for deployment
- Learn how to integrate other tools such as the EXBPA
- Configuring alerts and rules
- Measuring service levels
- Auditing Exchange permissions

EXC21: HELLO? IT'S FOR YOU! GETTING STARTED WITH UNIFIED COMMUNICATIONS
PAUL ROBICHAUX

Exchange 2007 and Office Communications Server 2007 offer some eye-popping unified communications features—but they're scary if your only telephony experience is with the phone on your desk. This session will explore the new features, demystify what they can do for you and your users, and provide practical deployment advice to help you get started right.

EXC11: IMPLEMENTING TLS IN EXCHANGE
CHRIS SCHARFF

Transport Layer Security (TLS) provides encryption for the transmission SMTP messages. Find out how to configure TLS in Exchange 2003 and 2007. Understand what this solution does and doesn't provide in terms of message security.

EXC03: OFFICE COMMUNICATIONS SERVER 2007 BRANCH OFFICE VOIP
ANTHONY VITNELL

Branch office telephony environments are typically costly to manage and remotely support. Office Communications Server 2007 provides the capabilities to deploy secure and reliable VOIP and Unified Communications capabilities to the branch office. This session will cover design and deployment scenarios using the Office Communications Server 2007 IP-PBX features in the branch office environment. Learn how easy it can be to deploy Unified Communications to a new branch office site with Office Communications Server 2007.

EXC19: POWERSHELL FOR BEGINNERS
PAUL ROBICHAUX

The Exchange Management Shell (EMS) is a key part of the Exchange 2007 experience. What if you're not a scripter? Don't worry; you can still get plenty done with EMS after just a little learning. This session covers the basics of what you need to know about how EMS works and what you can do with it.

EXC05: PROTECTING YOUR EXCHANGE 2007 FROM SPAM—BEST PRACTICES
DARAGH MORRISSEY

This session provides best practices to prevent spam hitting your Exchange 2007 deployment and covers the following areas:

- Spam terminology
- 1st/2nd/3rd generation techniques for blocking spam
- Best practices
- Reducing false positives
- Building a proof-of-concept to measure the performance of your anti-spam measures
- Overview of Exchange 2007 Edge Server anti-spam features
- HP case study

EXC12: USER PROVISIONING WITH POWERSHELL
CHRIS SCHARFF

A walkthrough of user provisioning using the flexibility provided with Windows PowerShell. Automate repetitive tasks to save time and reduce errors.

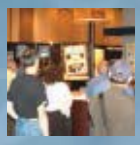
EXC09: WHAT'S NEW IN EXCHANGE 2007 SP1?
KIERAN MCCORRY

See Web site for session abstract.

DIVE INTO THE NEW RELEASES WITH MICROSOFT ARCHITECTS AND INDUSTRY EXPERTS!

WINDOWS SESSIONS
PRESENTED BY MICROSOFT

WINDOWS Connections 2007



Immerse yourself in the latest Windows technologies: **Windows Server 2008, virtualization, WDS, Windows Vista, SoftGrid** and more—**with experts from Microsoft Corporation and world-renowned subject magger experts!** Windows Connections offers the deepest and most relevant education for Microsoft Windows administrators—knowledge that is critical as major new products arrive for your enterprise.

Windows Server 2008 and **Windows Vista** introduce major change, and now is the time for you to quickly come up to speed. **Be prepared** through the real-world experience of our expert presenters and instructors. "Insider" details from Microsoft, MVPs, and other participants help you make sense of the new technologies, apply them to your environment, and master them faster and more effectively.

- Be fully prepared to deploy and support **Windows Vista**. Learn how to manage its advanced networking and security technologies, and how to support volume license activation (a major deployment hurdle if you're not ready). Learn all there is to know about new Group Policy settings and functionality from GPO guru Jeremy Moskowitz. Get a roadmap for how to manage and protect user data, from effective redirection and roaming to disk encryption. And get the inside scoop on Vista deployment and desktop management from experts Rhonda Layfield and Dan Holme.
- Become an expert on the soon-to-launch **Windows Server 2008**. Learn how to manage the GUI-less Server Core from command-line commando Mark Minasi, how and when to migrate to 32- and 64-bit versions of Microsoft's new server platform, and everything that's changed in server roles, including Active Directory security and disaster recovery. Discover how the new features of Terminal Services and SoftGrid can revolutionize the way you support applications in your enterprise. And get one-of-a-kind, practical guidance to securing your enterprise, from file share provisioning to event log auditing to using certificate-based authentication. And get the first of its kind insight into the new DFS Replication of Sysvol, and how to migrate your DCs to it.
- Take home **Solutions**: find out how to implement SharePoint document libraries as a replacement for shared folders, how to manage Windows for compliance and auditing, how to increase security though IPSec and network access protection, and how to implement role-based management and provisioning.
- This is the year of **virtualization** and **management.** Get the guidance you need to choose and implement a virtualization strategy with independent expert Alan Sugano's insights into VMware and Windows virtualization. And get up to speed with the new version of SMS: System Center Configuration Manager 2007.
- Become a more effective and efficient administrator through our unique **Windows PowerShell** courses.

PROTECTING SENSITIVE DATA WITH BITLOCKER DRIVE ENCRYPTION

This presentation will provide you with an overview of BitLocker™ Drive Encryption (BDE) including system requirements, features, and real-life examples of how to implement BitLocker™ to protect systems in a field office, to secure, upgrade, or decommission an existing drive, or to recover data from a compromised PC asset.

INTRODUCTION TO SERVER CORE RUNNING MINIMAL WINDOWS 2008

This session introduces the concept of Server Core. Server Core is a lightweight subset of Windows 2008 with roles specific to the Standard, Enterprise, and DataCenter environments that reduce the server's vulnerability to attack as well as the costs of upgrading and maintaining the server.

GETTING TO KNOW WINDOWS SERVER 2008—ADMINISTRATION, CLUSTERING, PERFORMANCE AND MORE

This session will introduce you to several new features in Windows Server 2008 including the new management console, new clustering features, performance and reliability monitoring, and a brief look at PowerShell. Windows Server 2008 includes some new and enhanced features to improve security and application deployment on your network. Enhancements in Terminal Services allow you to more easily deploy only the applications you want while protecting the server environment.

WINDOWS SERVER 2008 TERMINAL SERVICES TECHNICAL OVERVIEW

For organizations that have remote users, Windows Server 2008 adds improvements and innovations to Terminal Services that facilitate better integration of remote and local applications on client computers, access to these same remote programs via Web browser, and a means to access remote terminals and applications across firewalls. Because Windows Server 2008 will ship on x64, it has the ability to use the additional processors and RAM that x64 offers increasing the number of users that a Terminal Services server can support.

EVERYTHING YOU NEED TO KNOW ABOUT DEPLOYING VISTA IN 60 MINS

How many images do you currently maintain for your desktop deployments? How much time do you spend re-working those images when changes take place? This session will explain how to reduce the number of images you maintain as well as demonstrate how easy it is to maintain and update images using the BDD Workbench, Windows Automated Installation Kit, and Windows System Image Manager. There will also be a demo of the new ImageX utilities.

WHAT IS NETWORK ACCESS PROTECTION AND WHAT CAN IT DO FOR ME?

This session will introduce you to Network Access Protection (NAP), which is a new platform that ensures the health of your systems by performing computer health policy validation and many other processes. This session looks at NAP enforcement and the many enforcement options that can combine to ensure that you have healthy systems. Then it looks at how to enforce health polices for Dynamic Host Configuration Protocol (DHCP), Internet Protocol security (IPsec) as well as Routing and Remote Access (RRAS), and how it allows you to enforce health policies on VPN-based remote access connections to an intranet.

DEPLOYING IPSEC WITH WINDOWS VISTA

This session looks at the new network stack in Windows Vista. Innovations that help secure the network by filtering network traffic and prevent unwanted forwarding. This includes features in the Windows Firewall such as the new rules system, which has many scenarios already defined in an easy-to-use interface. You will also see how Windows Vista helps secure connections with tightly integrated Internet Protocol security and how this plays out in mixed networking environments.

WINDOWS SERVER 2008 VIRTUALIZATION—FEATURE AND ARCHITECTURE OVERVIEW

This session starts with an overview of virtualization technology discussing how virtualization technology is being embraced at the enterprise level, and the benefits it brings, including cost savings and more effective resource utilization. It also introduces Windows Server Virtualization, or WSv. WSv brings several advances to virtualization technology. This session talks about the business case for its use and introduces some of the technical and architecture details.

ACTIVE DIRECTORY

WIN721: ACTIVE DIRECTORY DISASTER RECOVERY IN WINDOWS SERVER 2008

GUIDO GRILLENMEIER

Backing up and restoring your complete Active Directory forest—or objects that you have accidentally deleted in a domain—has always been a lot of fun with previous versions of the Windows Server OS. Come to this session to find out how much more fun you can have restoring your AD or specific objects with Windows Server 2008! Microsoft has invested a lot of resources to completely overhaul the mechanisms and tools to back up Windows Servers in this OS release. This change has various impacts on the strategy you use to back up your AD Domain Controllers and how you restore them. It may even impact how you configure your domain controller disk subsystem. But there is a lot of good news when it comes to recovering objects in AD, which will be demonstrated in detail in this session. We'll also discuss those recovery tasks that remain to be a challenge.

WIN822: INCREASING THE SECURITY IN YOUR ACTIVE DIRECTORY USING WINDOWS SERVER 2008

GUIDO GRILLENMEIER

Active Directory has received various security updates in Windows Server 2008, some of which are hard to miss, such as the capability to deploy read-only domain controllers (RODC). However, there are plenty of other enhancements hiding under the hood that AD administrators should know about to further tighten the security in their AD infrastructures. This includes features such as Owner Access Restriction, fine-grained password policies, various updates around the auditing capabilities of Active Directory, and the Admin-Role Separation feature for read-only domain controllers (RODC). This session will explain how best to leverage the various new features to ensure the operation of a secure Active Directory with Windows Server 2008.

WIN823: REPLICATING SYSVOL IN WINDOWS SERVER 2008

RHONDA LAYFIELD

Replication of SYSVOL is one of the most important aspects when it comes to the security of your desktops. SYSVOL replicates all those group policy objects you have spent so much time researching/testing and ultimately implementing. But what happens when those settings never arrive at the desktop? In this session you will learn how SYSVOL is replicated and how to troubleshoot when it fails, step-by-step.

WIN712: WINDOWS SERVER 2008 ACTIVE DIRECTORY TECHNICAL DRILL-DOWN

MARK MINASI

Join Mark Minasi for a close-up look at Active Directory under Windows Server 2008. Find out about read-only domain controllers (they're more than just a BDC), fine-grained password policies, the new DCPROMO, and lots more!

SECURITY

WIN743: ARE PASSWORDS DEAD? LONG LIVE THE SMARTCARD

BRIAN KOMAR

The decision to enforce smart cards for authentication is a huge step for an organization. This session will look at the issues blocking smart card deployment in today's networks, help you plan a smart card deployment using Microsoft's Identity Lifecycle Manager 2007, and discuss a case study of a current implementation that Brian is working on.

WIN713: LAPTOP LOST—WHAT SHOULD I HAVE DONE, NOW THAT IT'S TOO LATE?

BRIAN KOMAR

Don't be the latest headline. Plug potential data "leaks" by encrypting user systems. Explore the pros and cons of Encrypting File System (EFS) and Windows Vista Bitlocker during this practical, technical session.

VIRTUALIZATION

WIN733: SOFTGRID 101

JEREMY MOSKOWITZ

Let me guess: your machines just "blow up" now and again. And I know why. It's because you have a zillion applications on them with a half a zillion conflicts and things just "deteriorate" over time. Wouldn't it be neat if you could just eliminate that problem altogether? Well, with Microsoft's newest acquisition, Softgrid, you can. It works by "wrapping up" your existing software into "sequences," and then putting them into a virtual sandbox. The upshot? Your applications aren't running "on" Windows. They're running within the sandbox. So, no more desktop deterioration. Softgrid is a big place, but come to this session to make sure you know the ins and outs before you get it in your organization!

Note: See the Virtualization pre-conference workshops on pages 15

WINDOWS SERVER 2008

WIN741: THE FILE SHARE IS DEAD: IMPLEMENTING WINDOWS SHAREPOINT SERVICES DOCUMENT LIBRARIES

DAN HOLME

After a short life of barely a decade, the Windows Server shared folder is dead, or at least on life support. Why? Because the features that we've all been missing—version control, version history, extensibility, and workflow—are now achievable using Windows SharePoint Services document libraries. Learn how to move forward into a new era of document management in this practical application of SharePoint.

WIN731: AUTOMATING AND PROVISIONING SECURE BUSINESS DATA SHARES

DAN HOLME

Whether for security, compliance, or manageability, the time has come for IT organizations to reexamine how they manage traditional file shares. This practical, solutions-focused session will present a vision for role-based, provisioned management of shared data folders. You will take away tools and a punch-list of processes that you can adapt to your enterprise's requirements to achieve that vision. Participants in this session are expected to have a solid understanding of access control lists (ACLs) and group management in Active Directory.

WIN832: 64-BIT WINDOWS SERVER 2008 VERSIONS—WHY SHOULD YOU CARE?

GUIDO GRILLENMEIER

By the end of 2007, the demand for 64-bit Windows servers will require all IT administrators to be aware of the ins and outs of 64-bit computing. Driven by the need to deploy the 64-bit Windows OS to support applications such as Exchange 2007, what are the challenges you'll face when moving down the 64-bit road: What does this mean for your 32-bit applications? Will they work and how? Will they perform better or worse? Should you leverage the x64 architecture or move to Itanium? What's really the difference between the two? How does Windows Server 2008 support either architecture? This session explains the most important things to know about the different 64-bit Windows architectures and why you should care about them. Special focus will be put on 32-bit compatibility challenges and solutions as well as discussing deployment scenarios for the 64-bit versions of Windows Server 2008.

WIN732: THE ACCIDENTAL DBA'S GUIDE: SQL SERVER EXPRESS AND MSDE FOR THE RELUCTANT

MARK MINASI

Think you're a network administrator but that you're not—or don't need to be—a SQL administrator? Think again; you may already BE a database administrator (DBA) and not even know it. Or... it might just be time to get ready to become one.

In the past few years, Microsoft has released tons of useful and free applications, management, and troubleshooting utilities. Tools like WSUS, Ultrasound, Windows SharePoint Services, Application Compatibility Toolkit, and others. While they're essential tools in any network, they've all got one thing in common: they need a real-live SQL Server to hold onto their data. Knowing that many folks can't afford a full-blown copy of SQL Server for those utilities, Microsoft has, for years, given away "cut-down" versions of SQL Server first called MSDE and more recently named SQL Server Express (SSX). In addition to these free Microsoft apps, many useful

third-party applications are built atop MSDE and SSX, and some of them install MSDE/SSX quietly—which, again, means that you may already be a DBA and not know it.

The bad news about these applications is that SQL administration skills are no longer optional: EVERY network admin has to know how to install, secure, and maintain simple SQL servers to serve as back-end for system utilities. But there's also good news: it doesn't take long to learn those skills. Join Mark Minasi, author of the best-selling "Mastering Windows Server" books and creator of "The Accidental DBA's Guide to MSDE and SSX," for a look at MSDE and SSX: how to install them, how to secure them, and how to run them, including 25 cookbooks to solve common problems and perform basic maintenance. If you need to understand MSDE/SSX to support SharePoint, WSUS, Ultrasound, ACT or any of the popular backup utilities built atop database servers, then this is the best time you can spend!

WIN821: COMMAND MICROSOFT WINDOWS FROM C: LEVEL... AND GET READY FOR SERVER CORE!

MARK MINASI

Still doing administration from the GUI? Well, that works, of course—but while GUIs are nice for now-and-then tasks, you can get a lot more done from the command line and, even better, you can stuff your favorite command lines into Notepad to create the world's simplest administration tool. But there are many more reasons to learn the command line. For one thing, text-based command interfaces like telnet, ssh, and the like run on virtually no bandwidth, which can be perfect in some remote-control situations. And then there's the reliable, largely unchanging nature of command-line tools: ask any Windows veteran how he got past having to learn the new Vista GUI to change an IP address, create a user, or change a password, and you're likely to hear that he just opened up a command prompt and used many of the the same "net" commands he'd been using since 1985. Perhaps the strongest argument for the command line, however, isn't the past—it's the future. Windows Server 2008 offers a sleeker, easier-to-control version of itself called "Server Core." It runs on less RAM and disk, but lacks a GUI. Once Windows Server 2008 ships, it'll be hip to be a command line square! The hard part, of course, is getting started—and who better to help you than Mark Minasi, whose 100+ "This Old Resource Kit" and "Windows Power Tools" columns have discovered and explained the best Microsoft command-line administrations tools for the past nine years. While the "altitude"—that is, high-level nature—of GUIs are nice, really getting the job in the least amount of time needs a more down-to-earth, "C:\>-level" approach. Join Mark when he covers over 50 Windows command-line tools and see how to "command" Windows to do your bidding!

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE. SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.

WIN842: MIGRATION STRATEGIES FOR WINDOWS SERVER 2008

SEAN DEUBY

Whether you're in the role of a single server administrator or owner of a corporate Active Directory, upgrading to Windows Server 2008 requires thorough planning and testing. This session will review different migration strategies for several Windows Server 2008 roles, with a focus on upgrading your Active Directory forest.

WINDOWS VISTA

WIN831: REIMAGINING THE MOBILITY AND AGILITY OF USER DATA: FOLDER REDIRECTION, ROAMING PROFILES, AND OFFLINE FILES

DAN HOLME

Windows Server 2003, Vista, and XP offer important functionality to ensure that data is available and secure. But until you start managing the intricacies of the technologies, your organization's data is difficult to access or take offline, challenging to protect, and intellectual property is exposed. In a worst-case scenario, critical user data is stored only on users' machines and is exposed to complete loss. Or, misguided corporate mandates lead too quickly to full-disk encryption. In this practical session, you will learn best practices for putting the pieces together: folder redirection, user profiles, offline files, encryption, Group Policy, ACLs, and shares. Participants are expected to have a very solid understanding of most or all of these technologies, or be ready to learn them offline. This advanced session prepares you to take away ready-to-implement, useful solutions to corralling, securing, and managing corporate data.

WIN711: GROUP POLICY IN VISTA: WHAT'S NEW – PART I (NEW GOODIES)

JEREMY MOSKOWITZ

Short answer: lots. So come hear the essential "What every admin absolutely needs to know" about Windows Vista and Group Policy. Learn why you need a Windows Vista management station. Learn how to get out of burning 5MB per GPO on each DC. Learn about the new things you can do (like power management and USB port management—only for Windows Vista clients. And, what's with the new acquisition of DesktopStandard? Will you see their products emblazoned with a Microsoft logo anytime soon? If you've got even one Windows Vista client that you're going to deploy, you positively must come to this session to learn the ropes from Jeremy Moskowitz, Group Policy MVP.

WIN712: GROUP POLICY IN VISTA: WHAT'S NEW—PART II (TROUBLESHOOTING)

JEREMY MOSKOWITZ

In Part II we'll discover how the beauty of Group Policy changes is not skin deep. There are some basic and detailed changes lying under the hood. And Jeremy Moskowitz of GPanswers.com and author of Group Policy: Management, Troubleshooting and Security is just the guy to bring it to you. In this session, you'll learn why you can't just run gpresult.exe anymore and get the results you want. You'll discover what happens if you reconnect to the network after a long absence. You'll learn how to crack open the new Vista event log and trace Group Policy flow to figure out what might be going on. You'll learn how other areas, like Offline Files and Group Policy Software Installation can be tweaked to give you just the information you need to fix what ails you. If you're looking for Group Policy answers to your troubleshooting questions, this is the session for you.

WIN723: EVERYTHING NEW IN VISTA AND SERVER EVENTS & EVENT LOGS

RHONDA LAYFIELD

Join Rhonda Layfield for an in-depth look at the overhauled event logs and eventing subsystems of Vista and Longhorn. Learn how to navigate the logs, consolidate, locate, and interpret events.

WIN843 PLANNING FOR WINDOWS SERVER 2008 AND VISTA LICENSING

SEAN DEUBY

Any rollout of Windows Server 2008 or Vista requires planning for Volume Activation 2.0. If you don't, your systems will grind to a halt a month after you've deployed them. You have to make a number of design decisions for your VA 2.0 infrastructure; this session will provide you with key information from practical experience to help you plan.

WIN833: AN INTRODUCTION TO SYSTEM CENTER CONFIGURATION MANAGER (SCCM) 2007 FOR NOVICES AND VETERANS

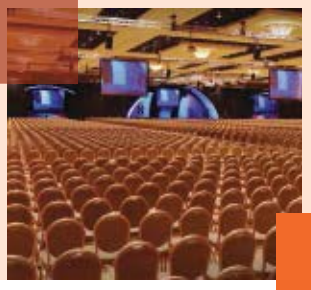
RHONDA LAYFIELD

Join Rhonda Layfield for a jump start to SCCM 2007. If you're new to the product, you'll learn what it takes to configure sites, collections, and packages. Find out how to deploy applications and configuration to your desktops. If you're a seasoned SMS veteran, you'll get the insight you need into the "delta"—what's new in SCCM 2007.

OFFICE & SHAREPOINT
SESSIONS PRESENTED BY MICROSOFT

Microsoft Office 2007:
Deployment Strategies and Techniques

The new Microsoft information worker platform is here: Microsoft Office 2007. Far more than just new versions of Word and Excel, Office 2007 is the new groupware client, information worker portal, and collaboration platform for Microsoft technologies. Leveraging server technologies in Windows, Exchange Server, and SharePoint Server, and based upon the advanced client platform technologies in Windows Vista, Office 2007 is simply a must-have new suite. Are you ready for it?



SharePoint Connections

SharePoint Connections is the essential conference for in-depth technical training on solution development and customization of Windows SharePoint Services and SharePoint Portal Server. SharePoint Connections is the largest independent conference for SharePoint developers and SharePoint IT professionals, and this conference will feature industry experts discussing development essentials, customization techniques, and developer case studies and end-to-end solutions that leverage other Microsoft technologies (including Outlook, InfoPath and Active Directory).

This targeted audience faces crucial purchasing decisions as they plan, deploy and customize secure, connected solutions for communicating and collaborating with employees, customers and partners using the SharePoint platform. The **SharePoint Connections** conference provides developers what they need to take their SharePoint deployments to the next level in order to achieve their corporate IT objectives.

MOSS 2007 SECURITY ENHANCEMENTS DEEP DIVE

This presentation delves into the significant new security features of Microsoft Office SharePoint Server (MOSS) 2007 including alternate authentication providers, native encryption, alternate access mapping and information rights management, and how to use these technologies to deploy SharePoint securely in both internal and customer-facing applications.

JUST WHAT THE HECK IS MICROSOFT OFFICE GROOVE 2007?!?

Groove 2007 is a new introduction to the Office suite of products that you can use to increase team collaboration and productivity. Groove can help you and your team work together more effectively and improve the quality of your deliverables. We will also see what security measures have been implemented which make Groove a more secure collaborative team workspace. We will examine a few of the more popular tools included with Groove 2007 along with other software that will help customize Groove workspaces.

HMS307: CAPACITY AND PERFORMANCE PLANNING FOR MICROSOFT SHAREPOINT PRODUCTS AND TECHNOLOGIES 2007

JAMES PETROSKY

This session covers techniques to determine Microsoft Office SharePoint Server 2007 capacity and performance needs, how to plan an architecture to meet those needs, and provides the steps required to conduct performance testing for Microsoft Office SharePoint Server 2007.

HMS206: DESIGNING AND BUILDING SOPHISTICATED COMPOSITE APPLICATIONS WITH MICROSOFT OFFICE SHAREPOINT DESIGNER 2007

JEROME THIEBAUD

Discover how to build sophisticated workflow-enabled composite Web applications on top of the SharePoint platform. This session explores how to build tracking and reporting applications accessing a wide variety of data sources using the power of the data view Web Part and Workflow Foundation. Also, learn how to apply customization to your SharePoint pages in a few clicks with modern tools such as master pages and CSS.

HMS309: HIGH AVAILABILITY AND DISASTER RECOVERY FOR MICROSOFT SHAREPOINT PRODUCTS AND TECHNOLOGIES 2007

JAMES PETROSKY

Learn best practices of data protection for your organization. This session covers the pros and cons of Windows SharePoint Services Backup/Restore, SQL-only backup/restore, SQL log-shipping, and the VSS writer. Also, learn how to take advantage of content recovery features, including the recycle bin, versioning, events, and fine-grained content migration.

HMS201: MICROSOFT OFFICE SHAREPOINT SERVER 2007 OVERVIEW

THOMAS RIZZO

Microsoft Office SharePoint Server 2007 is much more than an upgrade to SharePoint Portal Server (SPS) 2003 and Content Management Server 2002. This session covers technical fundamentals, feature overviews, new sets of server functionality, and implications for developers and IT professionals alike. NOTE: Since Office SharePoint Server 2007 is built on Windows SharePoint Services 3.0, we recommend that you also attend the "Windows SharePoint Services 3.0 Overview" session.

HMS204: MICROSOFT SHAREPOINT PRODUCTS AND TECHNOLOGIES 2007: ADMINISTRATIVE ARCHITECTURE AND PLANNING FOR DEPLOYMENT, PART 1

JOEL OLESON

This session describes the new deployment and administration architecture for Microsoft Windows SharePoint Services (WSS) version 3 and Microsoft Office SharePoint Server 2007. Learn about logical and physical design architectures, planning and deployment considerations, as well as inter-farm and intra-farm shared services capabilities. Also, understand the administration components and administration security considerations throughout the platform.

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE.
SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.

HMS305: MICROSOFT SHAREPOINT PRODUCTS AND TECHNOLOGIES 2007: DEPLOYMENT AND ADVANCED ADMINISTRATION TOPICS, PART 2

JOEL OLESON

This session is the second of a two-part series on deployment and administration in Microsoft Windows SharePoint Services (version 3) and Microsoft Office SharePoint Server 2007. Learn about advanced configurations and deployment architectures including extranet deployments and inter-farm shared services. Gain an understanding of steady state and advanced administration techniques and capabilities for the SharePoint farm including password management, disaster recovery, SQL management, patching and service pack management, and the Microsoft Common Engineering Criteria enhancements.

HMS202: MICROSOFT WINDOWS SHAREPOINT SERVICES 3.0 OVERVIEW

LAWRENCE LIU

Microsoft Windows SharePoint Services, a technology in Windows Server, provides the tools, infrastructure, and platform for the development of collaborative applications. Learn about the new features in Windows SharePoint Services 3.0 and how you can use them to make Windows SharePoint Services version 3.0 work for you.

HMS310: SEARCH IN MICROSOFT OFFICE SHAREPOINT SERVER 2007: CUSTOMIZING AND EXTENDING

THOMAS RIZZO

Enterprise Search is a critical piece of Microsoft Office SharePoint Server 2007. In this session we drill into the search technologies SharePoint offers, how to extend these search capabilities using custom user interfaces, and how to use the object model and Web services to add your search to your own custom applications.

HMS203: SHAREPOINT GOVERNANCE AND INFORMATION ARCHITECTURE GUIDANCE

JOEL OLESON

The most important thing you do to ensure a successful deployment is create an information architecture. Overlooking information management can lead to chaos. Come learn key SharePoint governance models that can help you balance the security and control that you need while continuing to support an easy-to-use, easy-to-manage platform.

CONFERENCE SESSIONS

OFF835: ACCESS AND SQL SERVER

ALISON BALTER

Access 2007 is an excellent client/server development tool. In this session, you'll learn when you should move an application to a SQL Server backend. This session will explore the options available to you when creating an Access client/server application. You'll learn how to upsize an Access database to SQL Server. Finally, you'll learn all of the tips and tricks that make your Access client/server applications optimized and fast!

OFF715: CUSTOMIZING AND DEPLOYING OFFICE 2007: THE REAL STORY

DAN HOLME

Join IT consultant Dan Holme for a truly independent, real-world alternative to Microsoft's song-and-dance about Office deployment. This session will help you cut your learning curve by giving you practical, take-away guidance to the tools and options available for customizing and deploying Office 2007 in your enterprise. Learn how to create an effective network installation point, create one or more customized installations, work with multilanguage environments, and deploy Office in a variety of scenarios. You will learn why Group Policy Software Installation is not a practical option for most organizations. And you will gain invaluable workarounds for blasting Office on to your users' computers without expensive third-party software management tools.

OFF735: FRONT-ENDING SHAREPOINT WITH ACCESS

ALISON BALTER

Access 2007 is tightly integrated with SharePoint. This session provides the attendee with everything that they need to know about working with Access 2007 and SharePoint. Topics covered include why SharePoint and Access 2007 are important tools within the organization, how to move your database to a SharePoint site, and how to open and work with SharePoint lists from within Access 2007. It will also cover how to integrate with the SharePoint workflow, how to work with SharePoint services offline, and how to map Access data to SharePoint data. All of these topics are necessary when integrating Access 2007 and SharePoint.

OFF745: MICROSOFT OFFICE POWERPOINT 2007: INTRODUCING AND SUPPORTING NEW FEATURES

DOUGLAS RYAN VANBENTHUYSEN

Microsoft Office PowerPoint 2007 offers an expanded array of features allowing users to create attractive presentations and to collaborate more readily on PowerPoint projects. This session will show the new features of PowerPoint, including the use of quick styles, to create logically designed graphical representations of bulleted lists, and how to use SharePoint slide libraries to share reusable content across an organization. The session will also address current top support issues.

OFF825: MICROSOFT OFFICE WORD 2007: CUSTOMIZING LOOK AND FEEL WITH TEMPLATES, STYLES, AND STYLE SETS

DOUGLAS RYAN VANBENTHUYSEN

Microsoft Office Word 2007 offers a variety of options to help you customize the look and feel of your documents. Out of the box, Word 2007 offers a variety of templates and style sets that allow you to quickly change the appearance of a document without the need to devote resources to coming up with a design. You can achieve further customization by building your own templates and creating your own styles and style sets. This session will explore the use of templates, styles, and style sets, including many new features such as Microsoft community submitted templates, defining custom font and color sets, and adding styles to the Ribbon interface.

OFF845: MICROSOFT OFFICE WORD 2007: REUSING CONTENT WITH BUILDING BLOCKS AND CITATIONS

DOUGLAS RYAN VANBENTHUYSEN

With Microsoft Office Word 2007, you have the ability to bring information and objects into your documents through building blocks and citations. This session will show how you can use building blocks to add objects to your documents, create building blocks of reusable content for distribution throughout an organization, and store reference information so you can easily add citations and source lists and make them available to other documents.

OFF725: WHAT'S NEW IN MICROSOFT ACCESS 2007?

ALISON BALTER

Access 2007 is dramatically different than its predecessors. This session will improve your productivity in Access 2007 by showing you all of the new and exciting tools that you can use to develop application. You not only will learn what has been added to Access 2007, you will also learn what has been taken away.

OFFICE & SHAREPOINT
CONFERENCE SESSIONS

HAD307: CUSTOMIZED SITE TEMPLATE AND DEFINITION MIGRATION
RICHARD TAYLOR

We all wanted it. We all needed it, but no one knew how. Microsoft wouldn't (or couldn't) tell us how. After stumbling around in the dark, we've figured it out! Come to this session to see how to perform a NON-vanilla migration with sites that have been customized with FrontPage 2003 and discover how to decipher the TechNet document on the subject.

HAD301: END-TO-END SOLUTIONS WITH THE 2007 RELEASE: DEVELOPING FOR IT PROS
DAVID GERHARDT

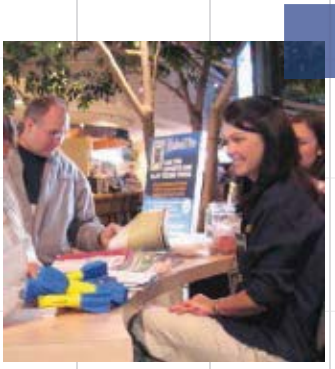
Review an end-to-end solution for a time-off request process. This session will show how to develop a form solution using Office Word 2007 in Office SharePoint Server 2007 without any custom code.

HAD203: EXPLORING THE NEW MICROSOFT FOREFRONT SECURITY FOR SHAREPOINT
MICHAEL NOEL

This session gives an overview of the new Forefront Security for SharePoint 2007 product, focusing on how the product can help to protect a SharePoint environment from traditional antivirus concerns as well as the latest threats. This session outlines specific best practice guidance on installing and configuring the Forefront Security for SharePoint product within an existing SharePoint environment and presents sample deployment scenarios. It also covers more in-depth information into some of the advanced functionality such as reporting and maintenance.

HAD308: FORMS AUTHENTICATION—HOW TO GET YOUR INTERNET-FACING MOSS SITE UP AND RUNNING
RICHARD TAYLOR

Forms-based authentication is an ASP.NET authentication service that enables applications to provide their own logon UI and do their own credential verification. If you have an anonymous Internet-facing site, you will want to know how to use Forms-based authentication.



HAD204: MONITORING A SHAREPOINT FARM USING SYSTEM CENTER OPERATIONS MANAGER 2007
MICHAEL NOEL

For several years, many administrators have found that the Microsoft Operations Manager (MOM) product is an ideal way to monitor the health and functionality of a SharePoint environment. Microsoft has further upped the ante with the release of the newest version of MOM, renamed as System Center Operations Manager (OpsManager) 2007. This session covers how you can use an OpsManager 2007 deployment to provide for proactive monitoring and management of a SharePoint 2007 environment. In addition to best-practice architecture and configuration advice for OpsManager, this session details the specific OpsManager Management packs for Windows SharePoint Services, SharePoint Server 2007, and Project Server 2007, discussing how you can use them for proactive, rather than reactive, administration of a SharePoint Farm.

HAD202: NO-CODE WORKFLOWS IN WSS V3
DUSTIN MILLER

Sending documents by e-mail for review is old and busted. In this session, you'll learn about the new hotness: built-in workflow features in WSS. See how easy it is to add intelligent serial and parallel workflows to documents and other SharePoint content, without writing a single line of code. There is a bonus, too: You'll get a glimpse into some of the other process management features in the new release of Office SharePoint Server 2007, such as information policies and records management.

HAD306: SHAREPOINT DIARIES
RICHARD TAYLOR

The benefits of a SharePoint implementation are great, but getting the point across to Executives is an even greater task. SharePoint is a complex product to explain to upper management; to get them to support you with the necessary resources will take careful thought, planning, and execution. Come to this session to learn how to present a proposal to the powers-that-be and at the same time ensure a successful SharePoint implementation as was outlined in REDMOND magazine by this author.

HAD305: VIRTUALIZING SHAREPOINT 2007 ARCHITECTURE
MICHAEL NOEL

Server virtualization technologies have taken front stage recently and many organizations have begun to seriously contemplate replacing physical servers, including SharePoint servers, with virtualization technologies. This session focuses on real-world architecture and best-practice recommendations for incorporating SharePoint architecture into virtualized environments running with either Microsoft's Virtual Server or EMC's VMWare Server products. The session focuses on outlining which specific components of SharePoint operate well in a virtualized environment versus which ones are not necessarily good candidates. In addition, this session gives an in-depth look at real-world designs for SharePoint using both major virtualization products and outlining the strengths and weaknesses of each product in relation to SharePoint functionality.

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE. SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.

PRE-CONFERENCE WORKSHOPS

11/4/2007

9AM–4PM • PRE-CONFERENCE WORKSHOP • EXCHANGE TRACK

EPR301: U-FIX-IT: TROUBLESHOOTING EXCHANGE SERVER 2007 (BRING YOUR OWN LAPTOP)

PETER O'DOWD

This intensive one-day troubleshooting workshop is essential for IT and Exchange administrators who want hands-on experience troubleshooting databases, message flow, and performance in a lab environment. Exchange expert and MVP Peter O'Dowd will walk you through the process of identifying and solving problems using a wide-range of tools and techniques. On your laptop, you'll perform virtual hands-on labs developed by Wadeware® that simulate problems, and then walk through the process of troubleshooting and solving them. Attend this full-day workshop to better understand Exchange database architecture and to gain knowledge necessary to recover and support your Exchange Server 2007 system.

NOTE: The laptop you bring MUST have at least 1 GB of memory and a DVD drive.

9AM–4PM • PRE-CONFERENCE WORKSHOP • POWERSHELL TRACK

PPR301: WINDOWS POWERSHELL: POWERFUL FUNDAMENTALS (BRING YOUR OWN LAPTOP)

DON JONES & JEFF HICKS

Master Windows PowerShell: Learn how to use the shell interactively (that's right, no scripting required) to perform key Windows administrative tasks. You'll learn all about PowerShell's object-oriented pipeline and learn how to manage services, run processes, and more. You'll also learn how PowerShell interfaces with Windows Management Instrumentation (WMI) and Active Directory Services Interface (ADSI) to extend your management reach to remote machines and into the directory. You'll learn all of the key PowerShell commands—called cmdlets—that enable core Windows administration tasks. You'll also learn to produce management and auditing reports using PowerShell's built-in filtering, grouping, sorting, exporting, and formatting capabilities. You'll even get a peek at PowerShell's built-in scripting language and capabilities, and learn all the tips and tricks for using PowerShell that you'll need to work faster and more efficiently. Bring your fully charged laptop with Windows PowerShell installed: You won't need it all day, but we'll have a special hands-on segment of our workshop that lets you experience and reinforce the PowerShell skills that you're learning.

NOTE: You must bring your own Windows XP or Windows Vista laptop, running Windows PowerShell v1.0 (from www.Microsoft.com/powershell). You must have local Administrator privileges. A licensed or free trial of SAPIEN PrimalScript Professional (from www.PrimalScript.com) is optional, but will be very helpful during class.
Not all segments of the day are hands-on, but significant hands-on exercises are included.

11/5/2007

9AM–4PM • PRE-CONFERENCE WORKSHOP • WINDOWS TRACK

WPR301: THE PERFECT DESKTOP: DEPLOYING AND MANAGING WINDOWS VISTA, WINDOWS XP, MICROSOFT OFFICE AND APPLICATIONS

RHONDA LAYFIELD & DAN HOLME (DAN PRESENTS IN THE AFTERNOON ONLY.)

In this fast-paced, intermediate to advanced session, Dan Holme and Rhonda Layfield will dive deep into the revolutionary new tools and technologies used to deploy Windows Vista, XP, Microsoft Office, applications, and configuration. You will learn best practices for the design, deployment, and maintenance of Windows clients and servers that can be supported effectively with application, security patch, and service pack rollouts into the future. You will take away a deployment methodology that works and a solid understanding of its functionality so that you can further refine the methodology to apply to your enterprise. Discover what you need to know to make them work: WinPE, ImageX, Windows Deployment Services (WDS), the Office Customization Tool (OCT), and the Solution Accelerator for Business Desktop Deployment (BDD).

9AM–4PM • PRE-CONFERENCE WORKSHOP • EXCHANGE TRACK

EPR302: WALK IN THE PARK: MICROSOFT EXCHANGE 2007 HANDS-ON LABS (BRING YOUR OWN LAPTOP)

PETER O'DOWD

Come take a six-hour guided tour of Exchange Server 2007 and see for yourself the next evolution of the world's most powerful messaging system. Experience the new Management Console, the five new server roles, e-mail policy enforcement and compliance, powerful new scripting tools, new architecture, new high availability and disaster recovery features, new mailbox features, and methods for migrating from earlier versions of Exchange. In this information-packed day you'll walk through several hands-on-labs developed by Wadeware® on your laptop with Exchange expert and MVP Peter O'Dowd, getting hands-on-experience with Exchange Server 2007.

NOTE: The laptop you bring MUST have at least 1 GB of memory and a DVD drive.

9AM–4PM • PRE-CONFERENCE WORKSHOP • POWERSHELL TRACK

PPR302: WINDOWS POWERSHELL: ADVANCED POWER (BRING YOUR OWN LAPTOP)

DON JONES & JEFF HICKS

Take PowerShell further, leveraging powerful built-in technologies for Windows and server administration. You'll learn all about PowerShell's built-in scripting language, and learn how to build powerful functions and filters that modularize script code into self-contained utilities. You'll get the details on PowerShell's scoping rules, learn to write error-handling routines, and learn everything about PowerShell script debugging, including the use of PowerShell's native debug mode. To keep you working efficiently, you'll receive a trial version of SAPIEN's award-winning PrimalScript visual development environment, which fully supports PowerShell script development. You'll also learn how to work with databases in PowerShell, and how to build simple graphical user interfaces, such as utility menus, right from within PowerShell. You'll even get a quick overview of PowerShell's extensible formatting and data type systems, giving you a foundation for additional independent research into these powerful areas for PowerShell extensions. Bring your fully charged laptop with Windows PowerShell installed: In the afternoon, you'll have a chance to put your new PowerShell scripting skills to use with a series of hands-on exercises.

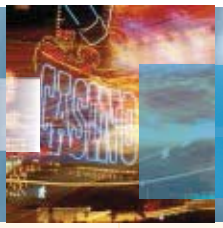
NOTE: You must bring your own Windows XP or Windows Vista laptop, running Windows PowerShell v1.0 (from www.Microsoft.com/powershell). You must have local Administrator privileges. A licensed or free trial of SAPIEN PrimalScript Professional (from www.PrimalScript.com) is optional, but will be very helpful during class.
Not all segments of the day are hands-on, but significant hands-on exercises are included.

9AM–12PM • PRE-CONFERENCE WORKSHOP • OFFICE/WINDOWS TRACK

OPRE01/WPRE06: MAKING THE MOST OF WINDOWS SHAREPOINT SERVICES AND MICROSOFT OFFICE

DAN HOLME

You've got Microsoft Office. You've got Windows SharePoint Services. Make the most of them! Join the guru behind www.OfficeSharePointPro.com for a three-hour workshop focused on how to leverage these two technologies in ways that add real value to your business. Learn what you and your information workers can do to maximize SharePoint lists, libraries, and content types. Discover what functionality differences to expect with the 2003 and 2007 versions of Office. And take away lots of practical, ready-to-implement guidance to ensure your SharePoint service is a success.



1PM–4PM • PRE-CONFERENCE WORKSHOP • WINDOWS TRACK

WPR02: GROUP POLICY ESSENTIALS: CONFIGURATION, CONTROL, AND SECURITY

JEREMY MOSKOWITZ

Group Policy is the most efficient way to manage desktops in a Windows environment. If you are still running to machines to install desktops, you are not taking full advantage of the power of Group Policy. In this practical workshop, Jeremy Moskowitz will help you gain control of your environment and get your life back. This is the perfect session to take before doing "deep dives" into the main sessions of the conference. You'll get a little bit of everything: deployment, configuration, control, and security ! We'll warm up with some Group Policy basics. Then, you'll learn how to get your XP and Vista client machines up and running with some new setup options. After your machines are up and running, Jeremy will show you how to manage your environment with templates, zap printers down to your computers, and remotely deploy software to your users' desktops. Finally, you'll learn how to use Group Policy to secure collections of machines. We'll examine how Group Policy can do the heavy lifting to the jobs you want to do! This session has both XP and Vista content.

Security!

9AM–12PM • PRE-CONFERENCE WORKSHOP • SECURITY TRACK

WPR306: DESKTOP SECURITY IN THE REAL WORLD

DEREK MELBER

Join Derek Melber for an in-depth exploration of some of the most important and sometimes complex areas of desktop management and security. The session will cover topics including imaging capabilities, application compatibility, and desktop management. New technology will be in Server 2008... there are key desktop security settings that will save you hundreds of manhours. We all know that security is at the forefront of our minds and responsibilities, so using WSUS, Group Policy, MBSA, etc. are essential for ensuring your desktops are secure.

We will also go over some of the most important settings and configurations that you can make to ensure your systems will be secure with the introduction of Vista into your organization. These technologies include PolicyMaker technologies and User Account Control... Do you have it turned on?

1PM–4PM • PRE-CONFERENCE WORKSHOP • SECURITY TRACK

WPR307: WINDOWS SECURITY, AUDITING, AND COMPLIANCE

DEREK MELBER

Dive into all aspects of Windows security from an audit and compliance standpoint. Derek Melber, renowned speaker and author of four books on the topic, will cover server and desktop security, as well as Active Directory and Group Policy security and delegation. Discover what Windows Server 2008 and Windows Vista offer your security initiatives. The focus of this workshop is beyond the mere configuration or implementation of security settings; rather, it is on how to successfully leverage auditing to discover and fix those areas that are not up to snuff for compliance.

Virtualization!

9AM–12PM • PRE-CONFERENCE WORKSHOP • VIRTUALIZATION TRACK

WPRE03: VIRTUALIZATION: A JUMP START

ALAN SUGANO

Virtualization is one of the hot topics this year. With significant increases in performance of the current generation of server hardware with quad-core processors, high memory capacity, and Serial Attached SCSI (SAS) drives, much of the processing power on a server goes unused. Virtualization allows you to take advantage of this processing power by running several virtualized servers on one physical host. If you're considering virtualization and are new to this technology, this workshop will get you up to speed on this technology. You'll learn about the following topics:

- Virtualization hardware. Server processors, memory, and hard drive configurations. Optimization of the hardware and the virtual environment for the best virtual guest performance. Running the x64 platform for virtual hosts and guests.
- Virtualization software (Virtual Server 2005, VMware Server, ESX Server).
- Backup strategies of virtual servers.
- Virtualization and high availability. Learn about the high availability solutions from Microsoft and VMware in the virtual server environment.
- Virtual guest limitations and how to determine if virtualization is a good fit for your application.

1PM–4PM • PRE-CONFERENCE WORKSHOP • VIRTUALIZATION TRACK

WPRE05: VIRTUALIZING MICROSOFT SERVER APPLICATIONS

ALAN SUGANO

Virtualization is a great technology, but how does it fit in with Microsoft Server Applications? This workshop will focus on SQL Server, Exchange 2007, and WSS 3.0/MOSS 2007 in a virtual environment. Each server application has different needs in a virtual environment. For each server application we will examine the following issues:

- To virtualize or not virtualize, this is the first question!
- 32- or 64-bit?
- Server configuration: Number of processors, type, memory, disk configuration, network cards, SAN type?
- What virtualization software should you use for your application?
- How do you configure guests for the best performance?
- How many users can you place on each virtual server?
- How many virtual guests can you place on a host?
- What are the High Availability Solutions for an environment?

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE.
SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.

POST-CONFERENCE WORKSHOPS

11/9/2007

9AM–4PM • POST-CONFERENCE WORKSHOP • EXCHANGE TRACK

EPS301: APPLYING SECURITY AND ENFORCING COMPLIANCE WITH EXCHANGE SERVER 2007 (BRING YOUR OWN LAPTOP)

PETER O'DOWD

Exchange messaging security is a giant topic, covering message access, encryption, retention, anti-spam, antivirus, and more. Add to that the powerful new compliance features of Exchange Server 2007 and you have an intensive one-day instructor-led workshop that will arm you with the knowledge necessary to secure your Exchange Server 2007 messaging system. Using virtual computers running on your laptop, you'll walk through several security and compliance labs developed by Wadeware® and led by Exchange expert and MVP Peter O'Dowd that will show you how to implement and work with the many new security and compliance features of Exchange Server 2007.

NOTE: The laptop you bring MUST have at least 1 GB of memory and a DVD drive.

9AM–4PM • POST-CONFERENCE WORKSHOP • WINDOWS TRACK

WPS301: CREATE A TEST ENVIRONMENT, VIRTUALLY AND INEXPENSIVELY (BRING YOUR OWN LAPTOP)

RHONDA LAYFIELD

Have you ever wanted a test environment but didn't know where or how to start? Purchasing new hardware to sacrifice to a test network can be pretty costly, not to mention the amount of time it takes to build and maintain the test environment. While this task can seem overwhelming, it doesn' t have to be. This workshop will give you hands-on experience in creating your very own test environment that mirrors your production environment with built-in disaster recovery! Now think about that for a second—regardless of the technology you require in your test lab, be it SQL, Exchange, Active Directory, or a development test environment, these step-by-step labs will work for all, and you get to perform them live. Attendees will need a CD drive, at least 1 GB of RAM and XP SP2 as their OS. Also download the latest version of VMware Workstation 30-day eval copy, which will be used to create your own virtual test environment live, in class. You will also be able to take these step-by-step labs back to work with you and create your own virtual test environment, no muss no fuss, and no drain on your budget!

9AM–12PM • POST-CONFERENCE WORKSHOP • OFFICE TRACK

OPR01: MAKING THE MOST OF MICROSOFT OFFICE

PHILIP WIEST

In this fast-paced, half-day event, you'll learn what you and your users can do to make more out of two ubiquitous Office applications: Outlook and Excel 2007.

OUTLOOK: What's the name of the program you use every day that when you open it says, "Look Out", er "Outlook"? If you've got more than 80 e-mails in your Inbox or unread mail promoting the release of Windows 2000, you're on your way to e-mail rehab. The workshop features Flags, Filters, Rules, and something we call Raiders of the Lost Archive. Teach your Users how to become e-mail savvy, e-mail efficient, and effective e-mail engineers.

EXCEL: You know there are some killer features in Microsoft Excel—you're just too overworked, underpaid, and busy putting out end-user fires to figure them out. Why not bring your staff something back from Vegas that they can actually use—like advanced Excel skills and techniques. Warning: What happens in this session doesn't have to stay in Vegas. You'll use these skills and techniques every day. This session features Fills, Formulas, and above all, fun. If you thought cells were only for celebrities, think again!

9AM–4PM • POST-CONFERENCE WORKSHOP • WINDOWS TRACK

WPS302: REIMAGINING IT ADMINISTRATION: ROLE-BASED MANAGEMENT, PROVISIONING, AND ACCELERATED ADMINISTRATION

DAN HOLME

Find out why this workshop, completely revised for Windows Server 2008 and Windows Vista, is consistently rated as a "best of breed" session, delivered as a capstone to your Windows Connections experience. From his work with thousands of IT professionals, from the CIOs of Fortune companies to front-line support professionals, Dan Holme has amassed a wealth of experience and expertise—solutions which enable you to deliver real-world best practices within the constraints of real-world budgets and technologies. This workshop will be invaluable for companies wanting to maximize their investment in their Windows infrastructure.

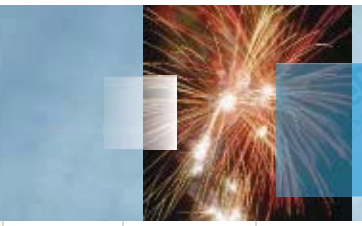
ACTIVE DIRECTORY EXTREME MAKEOVER: You will discover how to implement role-based management, in which users are defined by their business roles and where resource access and configuration are instantly, accurately, and auditably applied. Empower your enterprise to enable a documented, auditable structure for resource security, asset management, and more. Also learn how to implement a role-based AD administration model with a scripted, thoroughly documented delegation.

PROVISIONING: You have the technology. Your business has processes. But too commonly they are not aligned. Learn how concepts of provisioning can enable you to support business processes through easy-to-implement solutions for scenarios including user management, new and replaced computers, and group membership tracking, to name a few.

ACCELERATED ADMINISTRATION: Learn the tricks that Dan has developed with enterprises large and small to facilitate administration and security. Dan will focus on creating highly customized and effective MMC consoles, scripts, intranet pages, and toolsets utilizing the native Windows administrative tools, support tools, and Resource Kit and free third-party utilities.

Get in early! This workshop includes a sneak peek at solutions in Dan's new Windows Server 2008 Resource Kit book, "IT PRO SOLUTIONS KIT." Be sure to visit the Windows Connections Web site for the most up-to-date list of topics that will be covered in this workshop.

SESSIONS AND SPEAKERS ARE SUBJECT TO CHANGE.
SEE WEB SITE FOR UPDATES AND ADDITIONAL SESSIONS.



SPEAKERS
MICROSOFT AND INDUSTRY EXPERTS

SPEAKERS ARE SUBJECT TO CHANGE. SEE WEB SITE FOR UPDATES AND BIOS.

ALISON BALTER
INFO TECHNOLOGY PARTNERS

SEAN DEUBY
INTEL

DEVIN L. GANGER
3SHARP LLC

DAVID GERHARDT
3SHARP

GUIDO GRILLENMEIER
HP

JUERGEN HASSLAUER
HP

JEFF HICKS
SAPIEN TECHNOLOGIES

DAN HOLME
INTELLIEM
WINDOWS CONNECTIONS CONFERENCE CHAIR & OFFICE CONNECTIONS CONFERENCE CHAIR

DON JONES
SAPIEN TECHNOLOGIES, INC. & SCRIPTINGANSWERS.COM

BRIAN KOMAR
IDENTIT, INC.

RHONDA LAYFIELD
CONSULTANT/TRAINER

LAWRENCE LIU
MICROSOFT

ROMI MAHAJAN
MICROSOFT

JIM MCBEE
ITCS HAWAII

KIERAN MCCORRY
HP
MICROSOFT EXCHANGE CONNECTIONS CONFERENCE CO-CHAIR

DEREK MELBER
DESKTOPSTANDARD

MARK MINASI
MR&D

DARAGH MORRISSEY
HP

JEREMY MOSKOWITZ
MOSKOWITZ INC.

PETER O'DOWD
BLADE/WADEWARE

JOEL OLESON
MICROSOFT

TONY REDMOND
HP

STEVE RILEY
MICROSOFT

TOM RIZZO
MICROSOFT

PAUL ROBICHAUX
3SHARP
MICROSOFT EXCHANGE CONNECTIONS CONFERENCE CO-CHAIR

CHRIS SCHARFF
MESSAGEONE

ALAN SUGANO
ADS CONSULTING GROUP

DOUGLAS RYAN VANBENTHUYSEN
3SHARP

ANTHONY VITNELL
HP

PHILIP WIEST
PHWIEST & CO.

Check our Web site as we add more Microsoft and industry expert speakers.
www.WinConnections.com

Join us
IN LAS VEGAS FOR
CONNECTIONS 2007

LAS VEGAS, NEVADA

HOTEL ACCOMMODATIONS

Mandalay Bay Resort and Casino, 3950 Las Vegas Blvd. South, Las Vegas, Nevada, is the conference site and host hotel. SPACE IS LIMITED so reserve your room early by calling the conference hotline at 800-505-1201 or 203-268-3204.

* NOTE: ROOMS AT MANDALAY BAY HAVE BEEN TOTALLY REMODELED, VERY COOL! SPACE IS LIMITED • LAST YEAR ROOMS SOLD OUT EARLY SO BOOK YOUR ROOM TODAY!

AIRLINE

Please call Pericas Travel at 203-562-6668 for airline reservations.

CAR RENTAL

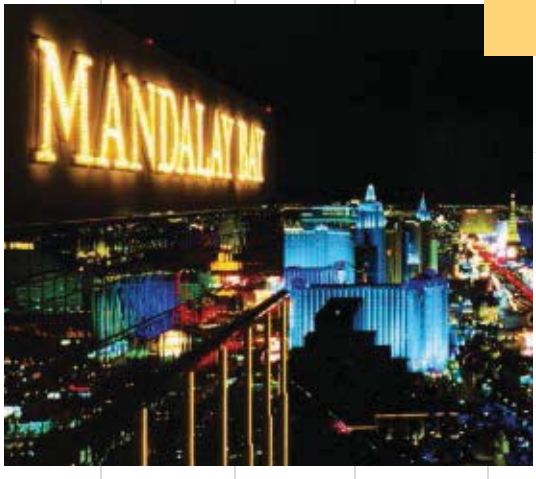
Hertz is offering auto rental discounts to attendees. Call the Hertz Meeting Desk at 800-654-2240 for reservations and refer to code CV# 010R0032 to receive your attendee discount.

ATTIRE

The recommended dress for the conference is casual and comfortable. Please bring along a sweater or jacket, as the ballrooms can get cool with the hotel's air conditioning.

SPONSORSHIP/EXHIBIT INFORMATION

For sponsorship information,
contact Rod Dunlap
480-917-3527 phone
E-mail rod@devconnections.com
See Web site for more details.
www.WinConnections.com



Network with your colleagues at Mandalay Bay Resort & Casino! There's so much to do, you'll never have to leave this 4-star resort!

- 11-acre tropical lagoon
- Sandy beach
- 3/4 mile lazy river
- 30,000 sq.ft. luxury spa and fitness center
- 16 restaurants on site, including The House of Blues
- 135,000 sq.ft. casino
- 12,000 seat sports/entertainment complex
- Shark Reef: Not your typical aquarium!

TAX DEDUCTION

Your attendance to a DevConnections conference may be tax deductible. Visit www.irs.ustreas.gov. Look for topic 513 - Educational Expenses. You may be able to deduct the conference fee if you undertake to (1) maintain or improve skills required in your present job; (2) fulfill an employment condition mandated by your employer to keep your salary, status, or job.

GROUP DISCOUNT

Register individuals from one company at the same time and receive a group discount.

1-3 registrants	$1,395 per person
Additional registrants after the 3rd (4th, 5th, 6th...)	$1,195 per person ($200 off each)

Call 800-505-1201 to take advantage of group discount pricing.

NOTES & POLICIES: The Conference Producers reserve the right to cancel the conference by refunding the registration fee. Producers can substitute speakers and topics and cancel sessions without notice or obligation. Updates will be posted on our Web site at www.WinConnections.com. Tape recording, photography is not allowed at any session. Conference producers will be taking candid pictures of events and reserve the right to reproduce. By attending this conference you agree to this policy. You may transfer this registration to a colleague. Please inform us if you have any special needs or dietary restrictions when you register. The conference registration includes a one-year print subscription to *Windows IT Pro*. Current subscribers will have an additional one year added to their subscription. Subscriptions outside of the United States and Canada will be digital. $25 of the funds will be allocated toward a subscription to *Windows IT Pro* ($49.95 value). **REGISTRATION & CANCELLATION POLICY:** Registrations are not confirmed until payment is received. Cancellations before September 20, 2007 must be received in writing and will be refunded minus a $100 processing fee. After September 20, 2007 cancellations and no shows are liable for full registration, it can be transferred to the next Connections conference within 12 months or to another person. Active Directory, Microsoft, MSDN, Outlook, Windows NT, Windows Server, Windows Vista, and Windows are either trademarks or registered trademarks of Microsoft Corporation. All other trademarks are property of their owners.

CONFERENCE REGISTRATION • NOVEMBER 5-8, 2007

FULL CONFERENCE REGISTRATION INCLUDES KEYNOTE ON NOVEMBER 5, 6:30PM, THROUGH CLOSING SESSION NOVEMBER 8, 4:30PM

NAME _____ PRIORITY CODE _____

COMPANY _____ TITLE _____

STREET ADDRESS (REQUIRED TO MAIL CONFIRMATION MATERIALS) _____

CITY, STATE, POSTAL CODE _____ COUNTRY _____

TELEPHONE _____ FAX _____ E-MAIL ADDRESS (IMPORTANT) _____

ONLINE
www.WinConnections.com

E-MAIL
info@devconnections.com

PHONE
(800) 505-1201, (203) 268-3204

FAX
(203) 261-3884

MAIL
Microsoft Exchange Connections 2007
Windows Connections 2007
Office Connections 2007
c/o Tech Conferences, Inc.
731 Main Street, Suite D-3
Monroe, CT 06468

❑ **Microsoft Exchange Connections** ..... on or before September 6, 2007 ..... $1295.00 _____
..... after September 6, 2007 ..... $1395.00 _____

❑ **Windows Connections** ..... on or before September 6, 2007 ..... $1295.00 _____
..... after September 6, 2007 ..... $1395.00 _____

❑ **Office Connections** ..... on or before September 6, 2007 ..... $1295.00 _____
..... after September 6, 2007 ..... $1395.00 _____

❑ **SharePoint Connections** ..... on or before September 6, 2007 ..... $1295.00 _____
..... after September 6, 2007 ..... $1395.00 _____

PRE-CONFERENCE WORKSHOPS SUNDAY, NOVEMBER 4, 2007 LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS.

❑ 9:00AM - 4:00PM U-Fix-It: Troubleshooting Exchange Server 2007 O'DOWD ..... $399 _____
❑ 9:00AM - 4:00PM Windows Powershell: Powerful Fundamentals JONES & HICKS ..... $399 _____

PRE-CONFERENCE WORKSHOPS MONDAY, NOVEMBER 5, 2007 LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS.

❑ 9:00AM - 4:00PM The Perfect Desktop ... LAYFIELD & HOLME ..... $399 _____
❑ 9:00AM - 4:00PM Walk in the Park: Microsoft Exchange 2007 Hands-on Labs O'DOWD ..... $399 _____
❑ 9:00AM - 4:00PM Windows PowerShell: Advanced Power JONES & HICKS ..... $399 _____
❑ 9:00AM - 12:00PM Making the Most of Windows SharePoint Services and Microsoft Office HOLME ..... $199 _____
❑ 1:00PM - 4:00PM Group Policy Essentials: Configuration, Control, and Security MOSKOWITZ ..... $199 _____
❑ 1:00PM - 4:00PM Desktop Security in the Real World MELBER ..... $199 _____
❑ 1:00PM - 4:00PM Windows Security, Auditing, and Compliance MELBER ..... $199 _____
❑ 9:00AM - 12:00PM Virtualization: A Jump Start SUGANO ..... $199 _____
❑ 1:00PM - 4:00PM Virtualizing Microsoft Server Applications SUGANO ..... $199 _____

POST-CONFERENCE WORKSHOPS FRIDAY, NOVEMBER 9, 2007 LUNCH IS INCLUDED WITH FULL DAY WORKSHOPS.

❑ 9:00AM - 4:00PM Applying Security and Enforcing Compliance with Exchange Server 2007 O'DOWD ..... $399 _____
❑ 9:00AM - 4:00PM Create a Test Environment, Virtually and Inexpensively LAYFIELD ..... $399 _____
❑ 9:00AM - 12:00PM Making the Most of Microsoft Office WIEST ..... $199 _____
❑ 9:00AM - 4:00PM Reimagining IT Administration ... HOLME ..... $399 _____

CONFERENCE MATERIALS

Full conference registration includes materials for the one conference for which you register. You may purchase materials for the other concurrently run events.

❑ Microsoft Exchange Connections Resource CD ..... $75 _____
❑ Windows Connections Resource CD ..... $75 _____
❑ SharePoint Connections Resource CD ..... $75 _____
❑ Office Connections Resource CD ..... $75 _____

PAYMENT TOTAL _____

*IMPORTANT: You must reference Microsoft Exchange Connections, Windows Connections, SharePoint Connections, or Office Connections on your check.

❑ CHECK (payable to Tech Conferences) All payments must be in US Currency. Checks must be drawn on a US bank.

❑ VISA ❑ MASTERCARD ❑ AMEX

CREDIT CARD NO. _____ EXPIRATION DATE _____

Cardholder's Signature _____ Cardholder's Name (print) _____

WinConnections 2007
c/o Tech Conferences, Inc.
731 Main Street, Suite C-3
Monroe, CT 06468

Mailroom: If addressee is no longer here,
please route to MIS Manager or Training Director

Listing 4: Defining Parameters

```
<FilterDescriptors>
  <FilterDescriptor Type="Comparison" Name="Key">
  <FilterDescriptor Type="Wildcard" Name="Name">
        <Properties>
                <Property Name="UsedForDisambiguation"
                  Type="System.Boolean">true</Property>
        </Properties>
  </FilterDescriptor>
  </FilterDescriptors>
  <Parameters>
        <Parameter Direction="In" Name="@MinActorId">
        <Parameter Direction="In" Name="@MaxActorId">
        <Parameter Direction="In" Name="@ActorName">
                <TypeDescriptor TypeName="System.String" AssociatedFilter="Name"
                  Name="ActorName">
                        <DefaultValues>
                </TypeDescriptor>
  </Parameter>
  <Parameter Direction="Return" Name="Actors">
        <TypeDescriptor TypeName="System.Data.IDataReader, System.Data,
          Version=2.0.3600.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"
          IsCollection="true" Name="ActorDataReader">
                <TypeDescriptors>
                        <TypeDescriptor TypeName="System.Data.IDataRecord,
                          System.Data, Version=2.0.3600.0, Culture=neutral,
                          PublicKeyToken=b77a5c561934e089" Name="ActorDataRecord">
                <TypeDescriptors>
                        <TypeDescriptor TypeName="System.Int32" IdentifierName="ActorId"
                          Name="ActorId">
                                <LocalizedDisplayNames>
                                        <LocalizedDisplayName LCID="1033">
                                          Id</LocalizedDisplayName>
                                </LocalizedDisplayNames>
                        </TypeDescriptor>
                        <TypeDescriptor TypeName="System.String" Name="ActorName">
                                <LocalizedDisplayNames>
                                        <LocalizedDisplayName LCID="1033">
                                          Name</LocalizedDisplayName>
                                </LocalizedDisplayNames>
                                <Properties>
                                        <Property Name="DisplayByDefault"
                                          Type="System.Boolean">true</Property>
                                </Properties>
                        </TypeDescriptor>
                        <TypeDescriptor TypeName="System.String" Name="WebLink" />
                        <TypeDescriptor TypeName="System.String" Name="Nationality" />
                        <TypeDescriptor TypeName="System.Int32" Name="Age" />
                </TypeDescriptors>
        </TypeDescriptor>
```

Services Provider Administration Web application, which is accessible through SharePoint Central Administration. The import analyzes the XML, verifies that it's conformant, and loads all the metadata definitions into the shared services database. Once this is complete, the entities within the shared services database are available for consumption by other parts of SharePoint (e.g., Web Parts, lists, user profiles, and search). Web Figure 1 shows the Actor entity as it appears in Shared Services Provider Administration after the ADF file has been successfully imported. The displayed fields are those that I defined in the ADF—and in this example, they correspond to all the fields in the source table—but it's up to the designer of the ADF to decide how much data to surface from the underlying source. You can also see the relationship I defined and the three actions. Next, let's see how this catalog of definitions can be consumed by other components such as Web Parts, lists, and search.

BDC Web Parts

Out of the box, you get six BDC Web Parts that you can use to display entities from the BDC. You can connect Web Parts to build very sophisticated Web pages. So let's see how we can use the Business Data List Web Part and Business Data Related List Web Part together.

The Business Data List Web Part lets you choose an entity from the catalog and display all instances of that entity in the back-end data source. It lets you filter the query on the back-end data based on the FilterDescriptors that are in the ADF file. You can also control the output by using a custom Extensible Style Language (XSL) style sheet. In our example, the Web Part displays the data in the section at the bottom left of Figure 3. I configured the Web Part to return every Actor entity rather than perform any filtering.

I can now use the Business Data Related Links Web Part to exploit the relationship I set up between the Actors and Movies databases in the ADF. When you configure the Related Links Web Part, you'll be able to see all the relationships that are defined in the BDC. Therefore, by choosing the ActorToMovie relationship, then using Web Part Connections to feed the selected actor into it, the movies will be associated with the selected actor. (After you define an entity in the catalog, it's accessible to many places, including a column in a list. So, when I defined the custom list that you see displayed in Figure 3, I specified the Actor column as being of type Business Data.) Next, you'll see a UI that lets you browse the catalog and select an entity that you want to display in that column. Recall that in the example, the default return value was the ActorName field so this is what's displayed. But you can choose to return whichever properties of an entity that you want. The data that's retrieved through the BDC is read-only, but it will be updated automatically when any of the writeable columns in the item are updated. This functionality lets you group custom data with data that exists elsewhere (and is probably currently only accessible through an LOB application). How powerful is that?

When you combine all the new features that SharePoint Search offers with the BDC, you can get similar results to what Web Figure 2 shows. You can see a separate tabbed search results landing page for actors with a pivot link for movies. When you select that link, you'll see another search results page showing all the movies that actor has appeared in.

Getting Down to Business

Do you have any data locked up in back-end business applications that you'd like to exploit? The BDC might be the answer. The BDC is a fantastic addition to SharePoint technologies, even though it's still immature with few support tools. I recommend you get familiar with the topics in the MOSS SDK. Armed with that information and a detailed knowledge about the back-end data, you'll be ready to fully exploit all your corporate LOB data.

InstantDoc ID 96772

Kevin Laahs
(kevin.laahs@hp.com) is a principal consultant in the HP Services Advanced Technology Group. He is coauthor of *Microsoft SharePoint Technologies: Planning, Design, and Implementation* (Digital Press).

Q: How can I set multiple start pages for Microsoft Internet Explorer (IE) 7.0 via the browser's graphical interface?

A: To configure IE to open multiple pages at browser startup, perform these steps:

1. Select Internet Options from the Tools menu.
2. Under the General tab, enter multiple URLs in the Home page box, as Figure 1 shows.
3. Click OK.

All these URLs will open when you launch IE.

InstantDoc ID 96836

—John Savill

Q: I keep hearing about application virtualization, especially with regard to Software Assurance (SA) and Enterprise Agreements. What's application virtualization and how does it relate to these licensing agreements?

A: Application virtualization lets you run applications locally on a computer without having to first install the actual application. Here's an outline of how application virtualization works.

On a special PC called the Application Sequencer, which is a clean OS build with no other applications installed, a special sequencing process monitors the installation of an application and tracks all changes made to the file system, registry, or services. It then writes this information to a single file data stream. The sequencer also executes the installed application to see which pieces of the data stream are needed to start the application.

A server is configured to place icons on the desktops, Start menus, or Quick Launch tool bars of application virtualization clients, which notifies the clients that a virtualized application is available.

If the user on the client machine clicks an icon that hasn't been clicked before, the application is streamed to the user's machine. Only the part of the stream that was marked as required to initiate the application (known as feature block 1) is sent and cached locally (so subsequent executions don't have to restream the data). This stream is then run inside a special environment known as the SystemGuard, which creates virtual file systems, registries, and other components, allowing the application to run without being installed, while protecting the underlying OS from any unwanted changes. However, you can save settings such as application configuration options, if so desired.

Why would you want this functionality? Imagine what you can do if applications execute in a contained, protected environment and don't interfere with each other. Compatibility problems vanish because applications don't know the other application is installed. Because compatibility problems are gone, developers can test applications much easier and faster, giving quicker time to market for

At a Glance

Q: In Windows Vista, how can I find all the files for which a user has access permissions?

A: You can use the Vista icacls command with the /findsid parameter to find all files that contain a specific SID in the file's ACL. The following example shows the command syntax:

```
ICACLS *.* /findsid savilltech\administrator /t /c
```

where /t means to perform the operation on the named directory and all subdirectories, and /c specifies that the operation continues on all file errors, although the error messages will still be displayed. You can also use the fsutil command, as follows:

```
fsutil file findbysid savilltech\john d:\documents
```

InstantDoc ID 96834

—John Savill

Figure 1: Setting multiple browser home pages

John Savill (jsavill@windowsitpro.com)

Mark Russinovich (mark.russinovich@microsoft.com)

Ask the Windows IT Pro Community

For answers to more of your Windows server and client systems questions, visit our online discussion forums at http://www.windowsitpro.com/forums.

new applications. And because applications aren't installed locally, the client machine is much cleaner and less likely to have problems.

So, what does this have to do with SA? Microsoft purchased Softricity, the maker of SoftGrid, which is the premier application virtualization tool. Instead of selling SoftGrid, Microsoft bundled it with three other products from companies Microsoft purchased and has made the bundle available as the Desktop Optimization Pack, which sells for $7 to $10 per desktop. That's very inexpensive considering that individually the products would cost hundreds of dollars. The catch is that only SA customers can buy the Desktop Optimization Pack, so essentially, Microsoft is using the pack as a way to get people to purchase SA.

Compatibility problems vanish because applications don't know the other application is installed.

InstantDoc ID 96835

—John Savill

The Case of the Unexpected PsList Error

This is a summary of a popular posting to Mark Russinovich's technical blog (https://blogs.technet.com/markrussinovich/about.aspx), which covers topics such as Windows troubleshooting, technologies, and security. You can read the entire post at https://blogs.technet.com/markrussinovich/archive/2007/07/09/1449341.aspx.

Not long after I deployed Windows Vista on my main desktop system, I noticed that a process became unresponsive and appeared to be consuming excessive amounts of CPU. I had a command prompt handy, so I ran PsList to dump detailed information about the process. (For more information about the PsList utility, go to http://www.microsoft.com/technet/sysinternals/utilities/pslist.mspx.) Instead of reporting a page full of statistics like I expected, however, PsList presented the error message *Failed to take process snapshot on MR-OPTERON.*

PsList obtains information from the system performance counters, which an application accesses using standard registry functions directed at the virtual HKEY_PERFORMANCE_DATA key, so the error message means that PsList was unable to query the virtual performance keys. When you point PsList at a remote system and don't have administrative rights on that system or the system isn't running the Remote Registry service, then PsList reports the same error, but I had never seen the message when using PsList to look at a local system. Something was different about Vista, and I set out to learn what.

Putting my original troubleshooting mission on hold, I launched Process Monitor (http://www.microsoft.com/technet/sysinternals/processesandthreads/processmonitor.mspx) and repeated the PsList command with Process Monitor looking on. I scanned the resulting trace looking for anomalous error codes, because when they're present they almost always point to the source of a problem, and found an access denied error.

For some reason, PsList, running as a standard user because I hadn't elevated the command prompt from which I ran it, was unable to open the PerfLib registry key for read access. I was perplexed because on Windows XP I had been able to run PsList as a standard user. I launched regedit, navigated to the key, and viewed its permissions. As I suspected, standard users aren't members of any of the groups the permissions grant access to.

I confirmed that to be the reason for PsList's failure by granting the Interactive Users group read access to the key and verifying that PsList subsequently worked. Now I was left with the question of which permissions XP assigns the key. I switched to an XP test system and viewed the key's permissions. Interactive Users have read access, explaining why PsList works as a standard user on XP systems.

I then pondered the reason for the change. The PerfLib key is where performance providers register their counters and DLLs, so when a tool such as PsList queries a counter, the performance API loads the associated DLL and calls functions in the DLL that return the desired data. Because the DLLs execute in the context of the process into which they load, they can't implement security that can't be easily circumvented by the process. It's therefore the responsibility of a performance data source, which might be the kernel or an application such as Microsoft IIS, to prevent unauthorized access to its performance data.

Preventing read access to the PerfLib key is therefore the equivalent of having a performance DLL implement security. Although locking down the key prevents the performance API from determining which counters are available and which DLLs provide performance data, with the exception of add-on applications, the core registrations are constant from system to system. That means that a process can circumvent any protection the locked-down key is attempting to provide by directly loading performance DLLs and calling their data functions.

To make a long story short, I filed a bug against Vista SP1 and Windows Server 2008 to have Interactive Users added back to PerfLib's permissions. The reliability and diagnostics team reported back that the permissions changed inadvertently during the release of Windows Server 2003, but I convinced them it didn't make sense, so inVista SP1 and Windows Server 2008 you won't need to edit PerfLib's permissions to be able to run tools like PsList as a standard user.

Another case closed by Process Monitor!

InstantDoc ID 96837

—Mark Russinovich

Counting on For

A Windows bug provides fine fodder for further For functionality

Last month, in "The Power of For" (InstantDoc ID 96539), I began a discussion about the For command, one of those little unsung Windows "hero" tools. I showed you how to use For to make a program capable of processing wild cards even when that program doesn't understand wild cards. For example, to make the imaginary Processfile command process every file whose name starts with "z," I could type

```
for %a in (z*) do processfile %a
```

In other words, For takes a program that processes one file at a time and transforms it into a program that can process a *series* of files—pretty useful functionality. However, last month I had room for only the merest of For's powers. Let's remedy that.

Couldn't Resist

A few years ago, Microsoft announced an entertaining bug—more like an Easter Egg—in the Windows Server 2003 and Windows 2000 Server versions of the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in. Open the snap-in, navigate to any group, right-click the group's icon, and choose Properties. In the resulting Properties dialog box, you'll see a Members tab that shows all the members of that group, including an androgynous head icon for each user. But if a group has more than 500 members, the hair color on the icon goes from black to white. Of course, when I heard about this bug, I *had* to try it out. But how would I generate 501 user accounts?

In previous columns, I've explained that you can create a user account on a domain from the command line by typing

```
net user <username> <password> /add /domain
```

However, typing a Net User command 501 times doesn't sound like fun. With For's /l option—which tells For to count—I can tell Windows to do 501 Net User reiterations in just one line. The syntax for For /l is

```
for /l %a in (<first number> <increment> <last
  number>) do <command>
```

For example,

```
for /l %a in (1 1 5) do echo %a
```

would have the effect of telling For to show the numbers 1 through 5, incrementing by one. Armed with this functionality, I can then type

```
for /l %a in (1 1 501) do net user testuser%a
  ComplexPassword$ /domain /add
```

This command creates 501 user accounts with the names testuser1, testuser2, and so on up to testuser501. Each user has the same password—*ComplexPassword$*—and the accounts are created on the domain. (Please try this only on a test domain.) After the command has completed, open the Active Directory Users and Computers snap-in, find the Domain Users group, and examine its membership: You'll find all white-haired icons.

To get rid of these test accounts, you can use the

```
net user <username> /delete /domain
```

command, but don't forget to use For to pump up its power to delete all 501 accounts, as follows:

```
for /l %a in (1 1 501) do net user testuser%a /domain
  /delete
```

Getting Complex

Thus far, the *command* portion of For has been a single command (e.g., Chml last month, Net User this month). But what if you want to perform multiple tasks in one For command?

For example, suppose you want to not only create a user named testuser*number* but also add that user to a domain local group called *test*. First, you can add a user to a domain local group with the command

```
net localgroup <groupname> <username> /add
```

To simultaneously instruct For to add the user to the *test* group, you can put the two necessary commands on a single line by placing the ampersand character (&) between them and surrounding the two commands with parentheses. To create 501 users, then, and also add each one to the *test* group, you could type

```
for /l %a in (1 1 501) do (net user testuser%a
  ComplexPassword$ /domain /add & net localgroup test
  testuser%a /add)
```

Stay tuned for more For!

InstantDoc ID 96704

Mark Minasi (http://www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 25 books, including *Administering Windows Vista Security: The Big Surprises* (Sybex). He writes and speaks around the world about Windows networking.

Did You Know?

You can meet Mark Minasi at the upcoming Windows Connections 2007 conference in Las Vegas, November 5–7. For more information, visit http://www.winconnections.com.

Steps to Get Started with Groove 2007

This "hidden" tool in Office 2007 can get your workgroups on the same page

Leave it to Microsoft to stick all kinds of new stuff in its Office suite and not tell anyone what it's good for. Microsoft Office InfoPath 2003 is a great example. InfoPath has been around since Microsoft Office 2003, but few people know why they should use it. With Office 2007, Microsoft Office Groove 2007 is the hidden tool that you might have but probably aren't taking advantage of. You can find out more about Groove and see some interesting demos on the Groove home page at http://office.microsoft.com/en-us/groove/fx100487641033.aspx. With a little knowledge, you can change Groove from an unused menu option to a powerful collaboration tool. These 10 tips will get you started.

1 **Create a Groove account**—Your first step is to create a Groove account. The Groove account is a file that defines your identity to Groove, defines the devices on which you'll run Groove, references the workspaces that you're a part of, and stores cryptographic information that secures your Groove data.

2 **Create a workspace**—The workspace is a shared area where people can actively participate on a project. You can create three types of Groove workspace: file sharing, where you share the contents of a folder across systems; standard, which contains a Files tool and a Discussion tool; and custom, where you select the tools to include. You can have multiple Groove workspaces, and each workspace can host different users and have different tools. You manage Groove workspaces by using the Workspace Explorer.

3 **Invite users to the workspace**—You add users to your workspace by using either the Groove Launchbar or the Workspace Explorer. In the Groove Launchbar, right-click the workspace you want to add a user to, then select the *Invite to Workspace* option from the pop-up menu. You can invite users to your workspace via email or IM.

4 **Add tools to the workspace**—Groove supplies 11 different tools that you can add to your Groove workspaces, including Calendar, Forms, Issue Tracking, Meetings, and SharePoint Files tools. There's even a chess game and drawing tools.

5 **Share files**—After you've set up your Groove workspace, you're ready to begin using it. Collaboration on shared documents is one of the most common Groove tasks. You set up document collaboration by using the Files tool. Click the Add Files button and browse to the files you want to add to the workspace. You can open any file listed in the workspace provided you have the application associated with it.

6 **Use chat**—Groove also supports an IM function (aka chat) that enables multiple users in a workspace to chat with each other. In addition to using chat for IM-style communications, you can also use chat to invite other Groove users to a workspace.

7 **Use alerts**—Groove alerts inform workspace members about changes to items in the workspace. Alerts are customizable, and they can take the form of text boxes or sounds. You customize Groove alerts in the Workspace Explorer by clicking the Workspaces drop-down list, then selecting the appropriate workspace and choosing the Set Alerts option.

8 **Work offline**—One of the most powerful features of Groove is that it allows you to work while connected or disconnected. If you've already created a Groove account on one system, such as your desktop, you can copy that account to another system, such as your laptop. You can make changes to the items in the workspace, then when you reconnect, Groove automatically synchronizes the changes between the two systems.

9 **Participate in discussions and meetings**—Groove also facilitates conducting group discussions and meetings. The Discussion tool enables group members to create topics and have threaded conversations. The Groove Meetings tool supports the creation of agendas as well as recording meeting minutes.

10 **Collaborate via SharePoint**—Groove features full integration with Windows SharePoint Services 3.0 through its SharePoint Files tool, which lets users collaborate on document libraries. SharePoint provides an effective central storage back end for when users are geographically distributed and must connect across the Internet.

InstantDoc ID 96775

Michael Otey (mikeo@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine* and coauthor of *SQL Server 2005 Developer's Guide* (Osborne/McGraw-Hill).

Jeff James (jjames@windowsitpro.com)
is senior editor, products, for *Windows IT Pro* and *SQL Server Magazine*.

At a Glance

Readers Review HOT PRODUCTS

Streamline Help Desk Management

Alloy Software's Alloy Navigator 5

I work at a small company, and nearly a third of the workforce works remotely. Our rapid growth drove the need for a better, more organized approach to IT governance. After researching the IT Infrastructure Library (ITIL) and tools that would let us implement some of ITIL's best practices, we tested four service management products and found that **Alloy Software**'s Alloy Navigator was the best platform for the money. One feature I like is that we can purchase only the asset modules we need and grow into the product's full capabilities over time.

Navigator was simple to install and went from development to production without major reconfiguration. One of our favorite features is that we can create business rules and customize them to match our business processes; another is the product's customizable data lists, which can be easily shared with IT staff. Whenever we had difficulty, Alloy's technical support team was responsive and thorough.

The software has a nice admin guide, but the documentation doesn't do a good job of explaining how powerful the product is. I made numerous support requests for new features to be added to future versions, only to find out that most of them already existed. On the negative side, the software recognition manager isn't the easiest to navigate and figure out, and the self-service Web site that's packaged with Navigator is a bit limited in its functionality.

—Jerry Millin, network manager

Reader:
Jerry Millin
Network manager
Product:
Alloy Navigator 5
Company:
Alloy Software
Contact:
http://www.alloy-software.com

Despite these shortcomings, I find Navigator to be a great product. We've increased our customer satisfaction by almost 30 percent while realizing an 85 percent reduction in monthly support calls. When we began using Navigator, we were averaging nearly 2,000 logged support incidents each month; now we log fewer than 300 and our freed-up Help desk staff has been able to take on more responsibilities. And Navigator still isn't fully implemented—our next step is to implement its change management capabilities.

Alloy Navigator is powerful and easy to use, and that's a combination that I don't often find in software products.

InstantDoc ID 96857

What's Hot continues on page 82

BEST BUY gift CARD

Wanted: Your Real-World Experiences with Products

Have you discovered a great product that saves you time and money? Do you use something you wouldn't wish on anyone? Tell the world in a review right here in What's Hot: Readers Review Hot Products. If we publish your opinion, we'll send you a Best Buy gift card! Send information about a product you use and whether it helps you or hinders you to whatshot@windowsitpro.com.

HOW WELL ARE YOUR SERVERS PROTECTED?

When it comes to disaster, it's not IF, but WHEN. And too often, it's when you least expect it.

Get High-Availabilty and Disaster Recovery "In-One" With Double-Take®. It is your job to keep servers up, data available and prevent downtime. Failure to protect mission critical data and applications can set your business back by weeks, months or worse. Disaster recovery is now one of the highest IT priorities.

In today's business climate, you have to have a tested plan and reliable tools in place for the moment your server (or site) goes down. Double-Take is that tool. Sold more than all other High-Availability tools combined, it is even certified for W2K Datacenter. No other HA tool is. A whole department sitting on their hands can cost thousands of dollars per minute. The ROI of Double-Take is a no-brainer.

Double-Take delivers real-time data replication combined with fail-over so you have high-availability and disaster recovery for your (virtual) Windows Servers -- safely and securely. This is the reason that hundreds of Fortune 500 companies worldwide use Double-Take to ensure their business continuity. Three levels of data compression allow more data to be replicated and increase performance and scalability.

Double-Take®

Double-Take gives you the peace of mind your data is safe and your job secure. Don't wait. *Download a free 30-day eval copy right now* and start protecting your data and applications.

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

Download your free eval copy today!

Sunbelt Software

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

Automate Security Monitoring

Security Laboratories' Security Recon

Reader:
Chris Marsh
Data security director

Product:
Security Recon

Company:
Security Laboratories

Contact:
http://www.securitylaboratories.com

Our IT environment has a large number of Windows servers, Active Directory domains, and Microsoft SQL Server database servers. As the security director for our organization, I'm charged with monitoring security processes and activities across the whole IT infrastructure. Historically, it's been difficult to ascertain what was going on on our network from a security perspective, then distill that information and analyze it from a central location. I'd been using a series of scripts and manual processes to format security data into something that could be reported and acted on. But over time, this approach to security monitoring and compliance proved to be unmanageable.

While I was trying to find a better solution, I came across Security Recon from **Security Laboratories**, and it seemed to be the right product to solve our monitoring, reporting, and compliance needs. After reviewing and testing the product I found it quite capable of solving our problems and providing us with a central Web-based console for analysis. The initial installation of Recon went smoothly, although some integration activities needed to be coordinated with our database group.

> "Security Recon has become a key player in our arsenal of security and auditing tools."—Chris Marsh, data security director

Recon's automated reporting function is one of the product's most appealing features. It lets us design reports that provide information on general or specific security violations, schedule the reports to run automatically, then provide that information to our IT staff via email. Another welcome feature, Access Profiling, lets us find out what system and network resources a given user or group has access to.

Recon's Help system was beneficial when we were trying to get the product installed and running, but it could be improved to provide additional operations guidance. Overall, Security Recon has become a key player in our arsenal of security and auditing tools.

What's Hot continues on page 84

Looking for a total website solution?

1&1 Home Package

3 months free!*

Offer expires October 31st.

	1&1 Home	Yahoo! STARTER	Go Daddy DELUXE
Included Domains	2 through contract duration	1	$1.99 per year with purchase
Web Space	120 GB	5 GB	100 GB
Monthly Transfer Volume	1,200 GB	200 GB	1,000 GB
E-mail Accounts	1,200 IMAP or POP3	200 POP3	1,000 POP3
Mailbox Size	2 GB	Unlimited	10 MB
Search Engine Submission	✓	✓	Extra charge applies
Website Builder	12 Pages	✓	Freeware
Photo Gallery	✓	✓	✓
RSS Feed Creator	✓	–	$4.99/month
Ad-free Blog	✓	✓	Freeware
90-Day Money Back Guarantee	✓	–	–
Support	24/7 Toll-free Phone, E-mail	24/7 Toll-free Phone, E-mail	24/7 Phone, E-mail
Price Per Month	$4.99	$11.95	$6.99
SPECIAL OFFER	3 months free!*	$8.96 first 2 months	Save 10% with 1 year contract
TOTAL/YEAR	$44.91	$137.42	$75.48

Act now and save!
Create your own .us domain. For a limited time, America's internet address is on sale.

.US

$2.99 first year

Offer expires October 31st.

Your complete website solution
Quickly and easily create an attractive website.
Order by October 31, 2007 and get 3 months free!

We offer a variety of hosting packages and servers to fit your needs and budget.

MEMBER OF united internet

Visit us now **1and1.com**

Or call **1.877.go1and1**

1&1

Efficiently Protect Against Malware

Sunbelt Software's CounterSpy Enterprise 2.0

Reader:
Jeff Breckon
Senior computer analyst

Product:
CounterSpy Enterprise 2.0

Company:
Sunbelt Software

Contact:
http://www.sunbelt-software.com

With my company's Web traffic growing, we began to experience a number of problems. Computers were slowing down and freezing up, and our current antivirus solution wasn't catching the common adware, spyware, and malware that was impacting the performance of those systems. We didn't want to place the responsibility for virus definition updates and virus scans on our users, so an enterprise antispyware solution became our highest priority.

We purchased **Sunbelt Software**'s CounterSpy Enterprise. Installing CounterSpy was ridiculously quick and simple, and there were no major configuration hassles. Originally we ran it on a high-end workstation rather than a server and it worked just fine. Most of the installation time was consumed by the deployment of CounterSpy agents to individual workstations. We had some trouble with an earlier version of CounterSpy that seemed to lock up some services, but version 2.0 seems to have fixed those problems.

"I can run a scan remotely and get the results to the proper support staff within minutes." —Jeff Breckon, senior computer analyst

CounterSpy has saved us quite a bit of time. Before we implemented it, if a machine at a remote site was running slowly or having problems, we'd have to dispatch a technician and that wasn't always a viable option. With CounterSpy I can run a scan remotely and get the results to the proper support staff within a matter of minutes. One thing that would make CounterSpy better is if there were a way to get information on a system during a scan while in the policy view mode.

Although CounterSpy isn't perfect, I wouldn't hesitate to suggest it to anyone in an organization that has a moderate number of workstations or workstations spread out over a fairly large geographical area.

InstantDoc ID 96857

DIRECTORY OF SERVICES

Windows IT Pro Network

Search our network of sites dedicated to hands-on technical information for IT professionals.

http://www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.

http://www.windowsitpro.com/forums

News

Check out the current news and information about Microsoft Windows technologies.

http://www.wininformant.com

EMAIL NEWSLETTERS

Get free NT/2000/XP/2003 news, commentary, and tips delivered automatically to your desktop.

- *Windows IT Pro UPDATE*
- *Vista UPDATE*
- *Windows Tips & Tricks UPDATE*
- *WinInfo Daily UPDATE*
- *.NET Briefing*
- *Exchange & Outlook UPDATE*
- *Scripting Central*
- *Security UPDATE*
- *SQL Server 2005 Express UPDATE*
- *SQL Server Magazine UPDATE*
- *Storage UPDATE*
- *Windows IT Library UPDATE*
- *Connected Home EXPRESS*

http://www.windowsitpro.com/email

PRO VIP ACCESS

Exchange & Outlook Pro VIP

Discover smart solutions for Exchange and Outlook administrators.

http://www.exchangeprovip.com

Scripting Pro VIP

Learn how to create more powerful scripts and get tips for automating those tedious administrative tasks.

http://www.scriptingprovip.com

Security Pro VIP

Discover practical, how-to advice for avoiding and solving security problems.

http://www.securityprovip.com

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles. Contact Joel Kirk at jkirk@penton.com.

Super CD/VIP

Get exclusive access to all of our print publications, including *Windows IT Pro,* via the new, banner-free VIP Web site.

http://www.windowsitpro.com/sub/vip

Article Archive CD

Access every article ever printed in *Windows IT Pro* magazine since September 1995 with this portable and speedy tool.

http://www.windowsitpro.com/sub/cd

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.

http://www.sqlmag.com

For detailed information about products in this issue of *Windows IT Pro*, visit the Web sites listed below.

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

SEND US YOUR INDUSTRY HUMOR! Email your funny screenshots, favorite end-user moments, and humorous IT-related pics to rumors@windowsitpro.com. If we use your submission, you'll receive a Ctrl+Alt+Del coffee mug.

ERROR Message ESL

I have many time to give

My name won't enjoy receiving this news

I will follow this instruction to achieve the desired result

Which platform did I needed to have installed?

SEND US YOUR END-USER STORIES

Ever have one of those days when users unintentionally tickle your funny bone? Ever NOT have one of those days?

We've published several hilarious end-user moments in this space over the past year, and we want to hear some more! In 150 words or fewer, send your greatest, funniest, most embarrassing user experience to rumors@windowsitpro.com, and we might just publish it on this page.

DILBERT® by Scott Adams

October 2007 issue no. 158, *Windows IT Pro* (ISSN 1552-3136) is published monthly. Subscriptions in US, $49.95 for one year; in Canada, $59 US currency, plus 7% for GST for one year; in UK £59; in all other countries, US $99. *Windows IT Pro,* 221 E. 29th St., Loveland, CO 80538, (800) 793-5697 or (970) 203-2782. Sales and Marketing Offices: 221 E. 29th St., Loveland, CO 80538. Advertising rates furnished upon request. Periodicals Class postage paid at Loveland, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,* P.O. Box 447, Loveland, CO 80539-0447. SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, P.O. Box 447, Loveland, CO 80539-0447. Printed in the USA. BPA Worldwide Membership Applied for May 2006.

Defragment Every Drive On Your Enterprise Without Leaving Your Chair

(Or even lifting a finger)

All New PerfectDisk 8.0!

PerfectDisk Command Center™
Perfection Made Automatic

Introducing

PerfectDisk 8 EVERYTHING FASTER

- **Centralized Management And Reporting**
- **Patent-pending Resource Saver™ Technology**
- **Exclusive Space Restoration™ Technology**
- **Exclusive AutoPilot Scheduling™**

RAXCO SOFTWARE

1-800-546-9728
www.raxco.com

Recognized as the world's most powerful defragmenter, PerfectDisk has always been the secret to faster, more reliable computers. Now, with a powerful new suite of enterprise tools, PerfectDisk 8.0 takes disk defragmentation to the farthest reaches of the enterprise, while placing total control right at your fingertips.

Are you sitting down? Good. Because with the PerfectDisk Command Center™ you can easily deploy, configure and manage the defragmentation of every system on the enterprise... all from the comfort of your own desktop. And that's just the beginning.

Our all new enterprise reports deliver valuable performance statistics and at-a-glance graphical displays that track and identify any fragmentation issue on any managed computer, and much more.

In addition, PerfectDisk's patent-pending Resource Saver™ technology finds file fragmentation without having to first open the file, further reducing any system impact of defragmentation. And new disk and CPU throttling provide even greater control over resources.

What's more, Raxco's exclusive AutoPilot Scheduling™ provides automatic defragmentation at the optimal time for each user. And AutoPilot Scheduling's Screen Saver Mode enables idle-time defragging at user-defined intervals. (There's really nothing to it.)

And features like our Single File Defrag and Consolidate Free Space Defrag (part of PerfectDisk's Space Restoration Technology™) are particularly valuable for users working with supersize files.

Give your users reason to stand up and cheer. And while PerfectDisk 8.0 is busy keeping each computer in tip top shape, you can sit back and simply take the credit. For the details and a free demo, visit

www.pdcommandcenter.com

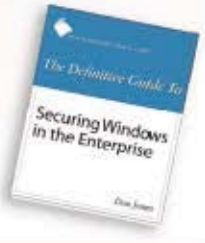
Microsoft GOLD CERTIFIED Partner

SECURITY EXPLORER®

Keep your security concerns under wraps with Security Explorer from ScriptLogic. Security Explorer simplifies the management of NTFS file and folder security, file shares, services, printer access, registry security and scheduled tasks, ensuring that access to privileged information is restricted on Windows servers and workstations.

- Centrally assess security using search criteria
- Add, modify, delete and clone permissions
- Backup and restore security as a separate data set
- New version 6.5 adds SharePoint security management

Download a 30-day evaluation today and get this Windows Security eBook free!



www.scriptlogic.com/coveryourdata

SCRIPTLOGIC®