

Windows Administration *in Realtime*

2 **Letter from the Editor**

Why the Vista Sour Grapes?

3 **Answers from the Experts**

Why Should I Start Looking at Server Core?

6 **Product Review**

NetPro NetControl for Exchange – Message Analysis

9 **Windows Vista Remote Server Administration Tools**

The Long-Awaited Administrative Tools Have Arrived

By: *Laura E. Hunter* - One of the challenges faced by early adopters of Windows Vista was the fact that administrative tools were not available. With the introduction of RSAT, Windows administrators now have the ability to deploy a fully functional administrative workstation. Explore the new features and functionality available through RSAT.

12 **The Deep Dive**

Give Vista a Chance!

By: *Greg Shields* - Are you taking others' word for it that "Vista sucks"? Consider confronting your fears and backing up your opinion with actual experience by taking the Realtime Give Vista a Chance Challenge.

15 **Practical PowerShell**

Local Account Management with PowerShell

By: *Jeffery Hicks* - Harness the power of PowerShell to easily discover what local user accounts are established on your member servers and desktops.

21 **Exclusively Exchange**

Moving to Exchange 2007 with a Little Help

By: *J. Peter Bruzzese* - Third-party tools that can help you move toward Exchange 2007.



SmartShedding[™] Technology

Allows the master outlet to sense when your computer has either been turned off or has gone into sleep mode, so it can shut off power to peripherals plugged into the controlled outlets—saving you power and money.

Your data should last forever. And so should our planet.

Save \$40* a year on your electric bill with the most efficient battery backup yet.

Let's protect what's important

What's in your computer? Photos, music, personal files, financial data, broadband access, videos, and more. Your computer has never been more important, and yet it has never been at higher risk for damaging power surges and other disturbances.

So like most people, you need to protect your assets. But like most people, you'd also like to protect the environment. With our new energy conscious products, you can do both. Energy efficient by design, our new smart products protect the power going in your computer, at a cost that is quickly offset by big energy savings. How? Not only do the new Back-UPS ES[®] and SurgeArrest[®] use power very wisely, they also boast a master/controlled outlets feature, which automatically powers down idle devices to conserve energy.

APC power protection products are available at:



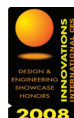
Office DEPOT

"The price tag on the new UPS is \$99.99. While I'm not in the habit of endorsing products in this blog, if you're in the market for a workstation-class UPS, why not opt for the greener option?"

- Heather Clancy
ZDNet.com

In fact, while protecting your power supply, we're up to 5 times more energy efficient than any other solution. By saving you \$40 a year in energy costs, our Back-UPS ES pays for itself in 2 short years. The high frequency, low copper design has a smaller transformer and environmental footprint. Even the packaging has been carefully selected and manufactured to maximize use of recycled materials and minimize waste.

In this world, every decision you make counts. So protect your power with a battery backup that works to protect the environment. It conserves power, it pays for itself, and it's backed by APC's 20-plus years of legendary reliability. For more information on this or our other great products, or for information about environmentally responsible disposal of your old battery, visit www.apc.com



Energy Efficient Solutions for Every Level of Protection:

Save \$25 per year* on your electric bill!

Surge Protection

Starting at \$34

Guaranteed protection from surges, spikes, and lightning.

7 outlets, Phone/Fax/Modem Protection, Master/Controlled Outlets

SurgeArrest[®]
P7GT



Save \$40 per year* on your electric bill!

Battery Back-UPS[®]

Starting at \$99

Our most energy efficient backup for home computers.

10 outlets, DSL and Coax protection, Master/Controlled Outlets, High Frequency Design, 70 minutes of runtime[†]

Back-UPS[®]
ES 750G



APC can help with your other power protection needs. Visit apc.com to see our complete line of innovative products.



Enter to Win a Back-UPS[®] ES 750G! (a \$99.99 Value)

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

Visit www.apc.com/promo Key Code c438w or Call 888.289.APC x9543 or Fax 401.788.2797

APC[®]
Legendary Reliability[®]

©2008 American Power Conversion Corporation. All rights reserved. All trademarks are the property of their respective owners.
e-mail: esupport@apc.com • 132 Fairgrounds Road, West Kingston, RI 02892 USA • 998-0968 [†]Runtimes may vary depending on load.

*Average savings are based on comparable competitive models, and are comprised of two energy saving features: An ultra efficient electrical design, and the master/controlled outlets feature.

Letter from the Editor

Why the Vista Sour Grapes?

by Greg Shields

If you've been keeping up with the Windows Server Community over the past month, you're familiar with my campaign to change the tide of negative Vista sentiment that is so prevalent in the media. Many organizations, even now over a year past Vista's release, are still playing the "wait-and-see" game when it comes to a Vista adoption.

From my experience, the source of this delay often originates from our community of Windows administrators. It is within our group of normally techno-philic individuals that Microsoft is losing the messaging war. We haven't been swayed by Vista's promise of compelling features. We are the ones turned off by the obvious omissions and application conflicts. And we are the ones that are ultimately telling our business leaders to wait by the sidelines.

That being said, Microsoft has had a few missteps in wooing interest and excitement from us Windows administrators. Unnecessary and cumbersome interface changes extend the new OS' learning curve. Remote administration tools such as RSAT took far too long to arrive. And great-on-paper-but-poor-in-implementation security mechanisms such as User Account Control resulted in more jokes than excitement. All these factors combine to make bad press out of what could be a good product.

But is our stubborn refusal to change only hurting ourselves in the long-run? Possibly. Later in this issue, I'll present some reasons why. There, I'll also introduce a challenge to the Vista-haters. Keep your eyes peeled.

Also in this issue, Don reviews NetPro's NetControl for Exchange Message Statistics, Peter talks about the transition from Exchange 2003 to 2007, Jeff gives us details on antivirus reporting using PowerShell, and Laura Hunter writes up an excellent feature on those Remote Server Administration Tools we've all been waiting for.

Keep us in the know about your Vista upgrade decision process. Are you the gatekeeper for getting new technology in your business? Have you made the jump? Or do you think the decision to wait will haunt you down the road? Let us know at feedback@realtimepublishers.com. ♦

Answers from the Experts

Why Should I Start Looking at Server Core?

by Don Jones

Q: Windows Server 2008's Server Core option seems limited and there are some barriers to including it in our organization because it doesn't offer antivirus software. Why should I start looking at Server Core?

A: This is a debate that fellow columnist Greg Shields and I have been having for a few months. I'll start with your point about antivirus software, and

simply say that, while at this point there are no antivirus applications designed specifically for Server Core, there's nothing stopping the major manufacturers from offering such software. It's probably just a matter of time before it starts appearing. That said, keep in mind that Server Core runs an extremely limited set of applications; unless you're using it as a file server (where it would be storing many files, of course), you could easily

use Software Restriction Policies (SRPs, a portion of Group Policy) to simply prohibit the execution of any executables except those intended to run on Server Core. Even as a file server, you could easily have scans performed by another server—this is an especially common scenario in some organizations, where a single server is dedicated to scan all the organization's shared folders.

World's hottest IT topics

Windows PowerShell™: TFM® 2nd Edition
Windows PowerShell™: TFM® 3rd Edition
(covers Windows PowerShell v2.0)
ADSI Scripting: TFM®
WSH and VBScript Core: TFM®
PrimalScript 2007: TFM®
Windows Server 2008: What's New/What's Changed
Exchange Management Shell TFM®
Managing Active Directory Windows PowerShell TFM®



For more information:
www.sapienpress.com



But understand that that Server Core is not a panacea for all your server needs. My suggestion is to start looking at infrastructure servers first: Machines that only handle domain controller, DHCP server, and DNS server roles. Upgrade them to Windows Server 2008 Server Core first to benefit from lowered patch management requirements, a smaller footprint, and an inherently more secure platform—which is just as manageable as the “full” server product. Consider file servers next, after you’ve conquered the antivirus problem. Finally, look at Web servers. Realizing that Server Core is useful only for Web servers that need Classic ASP, completely static, or perhaps PHP-based Web sites

(and the majority of PHP Web sites certainly aren’t running Windows, let alone IIS), your use of Server Core as a Web server may wind up being pretty limited.

You might even reserve Server Core for new server deployments, such as new domain controllers. One reason I like Server Core as an upgrade for existing infrastructure servers, though, is that it allows you to get a somewhat lower-powered server—perhaps 1U rack machines with a good amount of RAM and relatively little disk space—in place for infrastructure purposes, freeing up larger machines that had been performing those tasks. Server Core is also a perfect choice for branch office infrastructure servers: Make

them a Read-Only Domain Controller (RODC), perhaps, add DNS and DHCP, and you’ve got a small, low-maintenance server that’s perfect for deployment to remote offices without a significant IT staff. ♦

Do you have an IT question you’d like answered? Send your question to answers@realtimepublishers.com. We cannot provide personal replies but will select questions with broadest appeal for inclusion in a future issue.

Don Jones is a Series Editor for Realtime Publishers, and the Director of Training and Publishing for SAPIEN Technologies. Visit him online at www.ScriptingAnswers.com.



Read an excerpt from the new Quest Software white paper *"Be the Master of Your Domain – Understanding Windows Server 2008 Active Directory Domain Services."*

—by Tony Murray.
Directory Services MVP

Microsoft recently announced the release of Windows Server 2008 RTM. Codenamed "Longhorn," this latest version of the server operating system from Microsoft marks a significant departure from its predecessors. This white paper introduces the changes made to Active Directory in Windows Server 2008 and addresses the impact for organizations with Active Directory already installed.

New Forest and Domain Functional Level

In Windows Server 2003, Microsoft allowed administrators to set the functional level of the domain or forest to a specific value, assuming certain conditions were met. The available AD functionality was determined by the functional level. For example, a Domain Functional Level of 2 (Windows Server 2003) permitted domain controller renames, updated and replicated last logon time stamp attribute and certain other features not available with other levels. Similarly, a Forest Functional Level of 2 allowed for cross-forest trusts, domain renames, and so on. Windows Server 2008 provides a new level: 3 (also known as Windows Server 2008).

Domain Functional Level 3

Domain Functional Level 3 provides the following features:

- All features from the Windows Server 2003 domain functional level
- Distributed File System Replication support

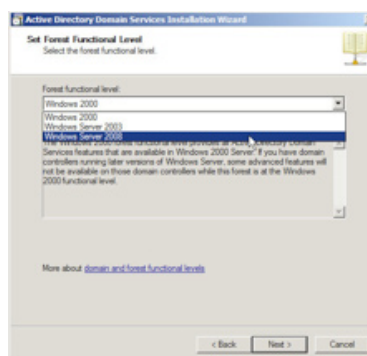
for SYSVOL, which provides more robust and detailed replication of SYSVOL contents

- Advanced Encryption Services (AES 128 and 256) support for the Kerberos protocol
- Last Interactive Logon Information, which displays the time of the last successful interactive logon for a user, the workstation used, and the number of failed logon attempts since the last logon
- Fine-grained password policies, which make it possible for password and account lockout policies to be specified for users and global security groups in a domain

Forest Functional Level 3

Forest Functional Level 3 provides all the features available at the Windows Server 2003 forest functional level, but no additional features. The sole purpose of raising the forest functional level to 3 is to prevent any new downstream domains or domain controllers from being joined to the forest.

One other item to note is that Windows Server 2008 domain controllers can be added to domains at Functional Level 2 (i.e., Windows Server 2003). If your organization has an urgent need for read-only domain controllers (RODCs), you can deploy them into your existing Windows Server 2003 forest without having to first upgrade your existing domain controllers.



Read-only Domain Controller (RODC)

The introduction of the RODC in Windows Server 2008 may represent the biggest change to AD since its Windows 2000 inception. The RODC is intended to reduce the risk of security compromises in locations where the threat is

highest (such as a perimeter network) or where the physical security of the domain controller is not optimal (for example, a branch office).

Unlike standard domain controllers (called writable domain controllers), the RODC does not replicate any changes to other domain controllers. This means that an attacker cannot use a compromised RODC to gain control of the forest by replicating permissions or schema changes. An attacker would be limited to using a compromised RODC to gain access to data held within the local credential cache. To reduce this risk, administrators have the ability to configure the RODC to cache only the password hashes of the accounts that will actually use the RODC for authentication.

The risk of compromises can be reduced even further by installing the RODC in combination with the Server Core version of Windows Server 2008. This effectively lowers the surface area for attack and reduces the patching requirements.

The RODC also supports the filtered attribute set, a new feature that enables administrators to define a set of attributes with values that do not replicate to RODCs in the forest. An example would be an application that uses certain attributes to store credential information for authentication to the application. If these attributes are added to the filtered attribute set, their values are replicated between writable domain controllers as normal, but they are not replicated to your RODCs.

About Quest Software, Inc.

Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases, Windows infrastructure and virtual environments. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 90,000 customers worldwide meet higher expectations for enterprise IT. Quest Software can be found in offices around the globe and at www.quest.com.

Want more? Read the entire white paper at www.quest.com/GetActive

Product Review

NetPro NetControl for Exchange – Message Analysis

by Don Jones

As great a product as Exchange Server is, there are a few critical capabilities that enterprises simply need, and which Exchange by itself can't provide. That's spawned a rich ecosystem of third-party products, and directory services expert NetPro is the latest to join the Exchange fray with NetControl for Exchange – Message Analysis.

Service-Oriented Architecture

First, a word about NetPro's NetControl architecture. Designed as a Service-Oriented Architecture (SOA), NetControl is intended to address the problem that many third-party software vendors introduce into an environment, primarily the problem of deploying and maintaining software agents. With NetControl, you start by installing the NetControl Console, a sort of central management interface that serves a similar purpose to the Microsoft Management Console (MMC).

The NetControl Console is where you install what I call capabilities, such as the Message Analysis piece. You use the Console to designate other servers to handle the workload of collecting message statistics and information—these don't need to be Exchange servers, but they do need to have LAN-quality connectivity to your Exchange servers—and the Console takes over. It deploys the necessary agent modules to the servers you designate, tells them when to perform their designated tasks, and even makes sure that the agent software stays up-to-date. This is accomplished by means of a generic "NetControl" agent on each remote server; this generic agent knows to contact the Console from time to time to download new agent modules and to update its workload schedule. The Console provides other shared capabilities, including data storage, workflow management, reporting, and so forth. Other NetPro products also integrate with this NetControl architecture, so if you're using more than one, you start to see major benefits in terms of maintenance and operations.

Message Analysis

The main job of Message Analysis is to continuously analyze your Exchange message stores and not only collect statistics but also generate a comprehensive search index of individual messages. Once gathered, this data enables three major scenarios:

- ▶ **Statistics reporting.** Reports can be as simple—and useful—as storage trend analysis, helping you to see what message stores are doing in terms of growth. You can create more complicated reports, too, including complete and detailed organizational chargeback reports, helping to allocate the cost of the messaging infrastructure across your company's departments based on their actual use of the system.
- ▶ **Troubleshooting.** Because the system tracks detailed statistics about message flow, you can generate various reports that help troubleshoot poor performance or outright problems in the infrastructure.

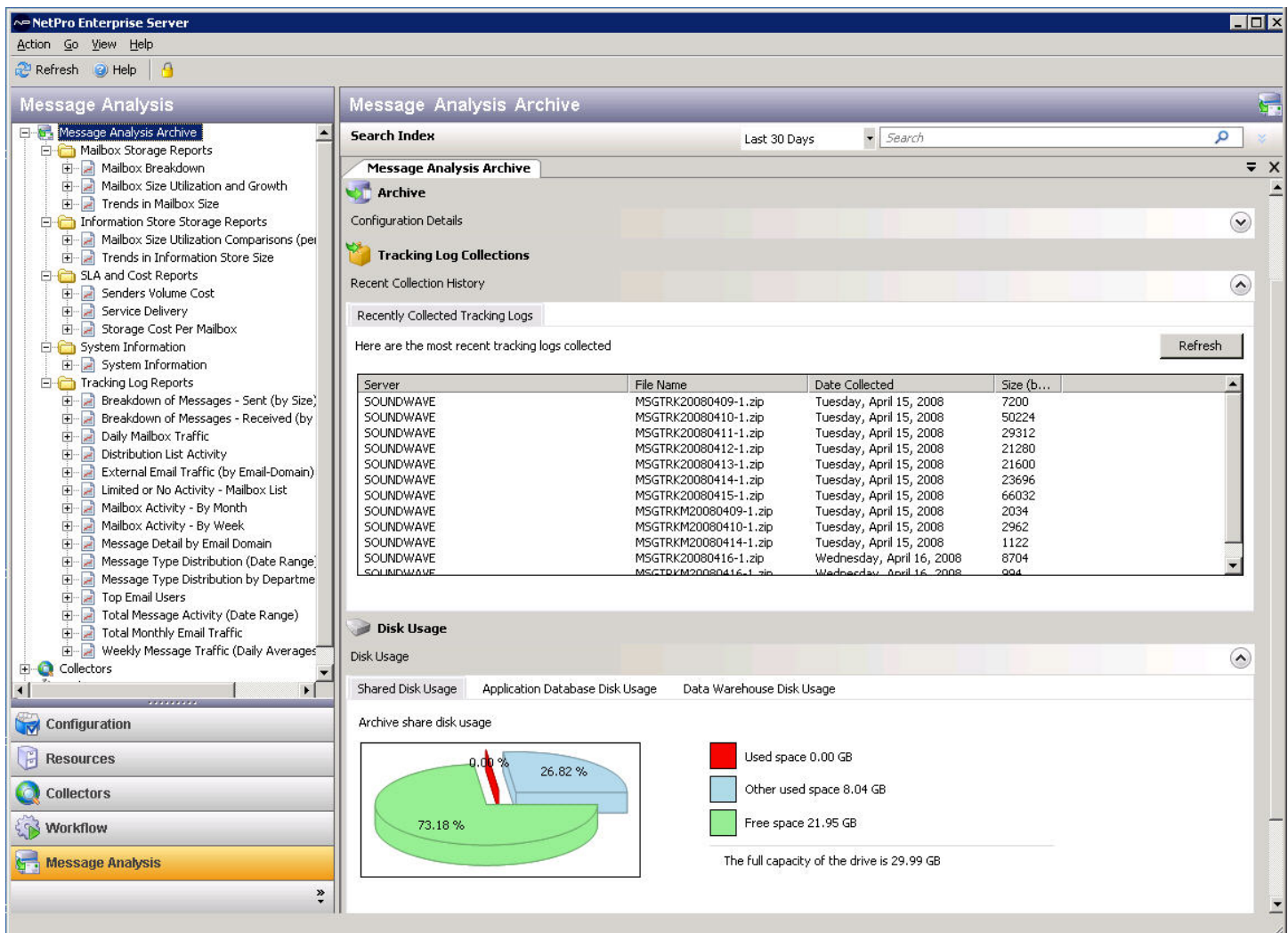


Figure 1

- **Message searching.** This provides a Windows Desktop Search-like interface where you can search for messages using all kinds of criteria—dates, recipients, keywords, and more. This is a crucial capability for organizations dealing with compliance requirements or working on e-discovery for legal proceedings. The system fully respects Exchange security so that unauthorized administrators can't use search to gain access to messages they shouldn't. In addition, it's designed to work quickly using an index of messages rather than having to touch individual message stores directly.

Obviously, these three major categories break down into hundreds of potentially useful production tasks. Because much of the benefit comes from reports, the tool uses NetControl's shared reporting architecture to provide a lot of bundled reports, along with automated report scheduling and delivery (actually, NetControl itself utilizes SQL Server Reporting Services (SRS), which provides a lot of these capabilities in a very standardized fashion).

Impressions

NetControl is almost ridiculously easy to install—no more difficult, say, than installing a small software application and less complex than even a custom Office install. Designating servers to handle the Message Analysis workload is equally straightforward—just enter some server names and you're done. Once designated to handle the analysis workload, the system works pretty much automatically. Within a day, I was able to start running reports against a fairly sizable set of Exchange message stores that I use in my lab. Something I hadn't fully appreciated was the fact that the tool is gathering statistics from *all* Exchange servers into a single, consolidated log—using the tracking reports, I was able to actually follow

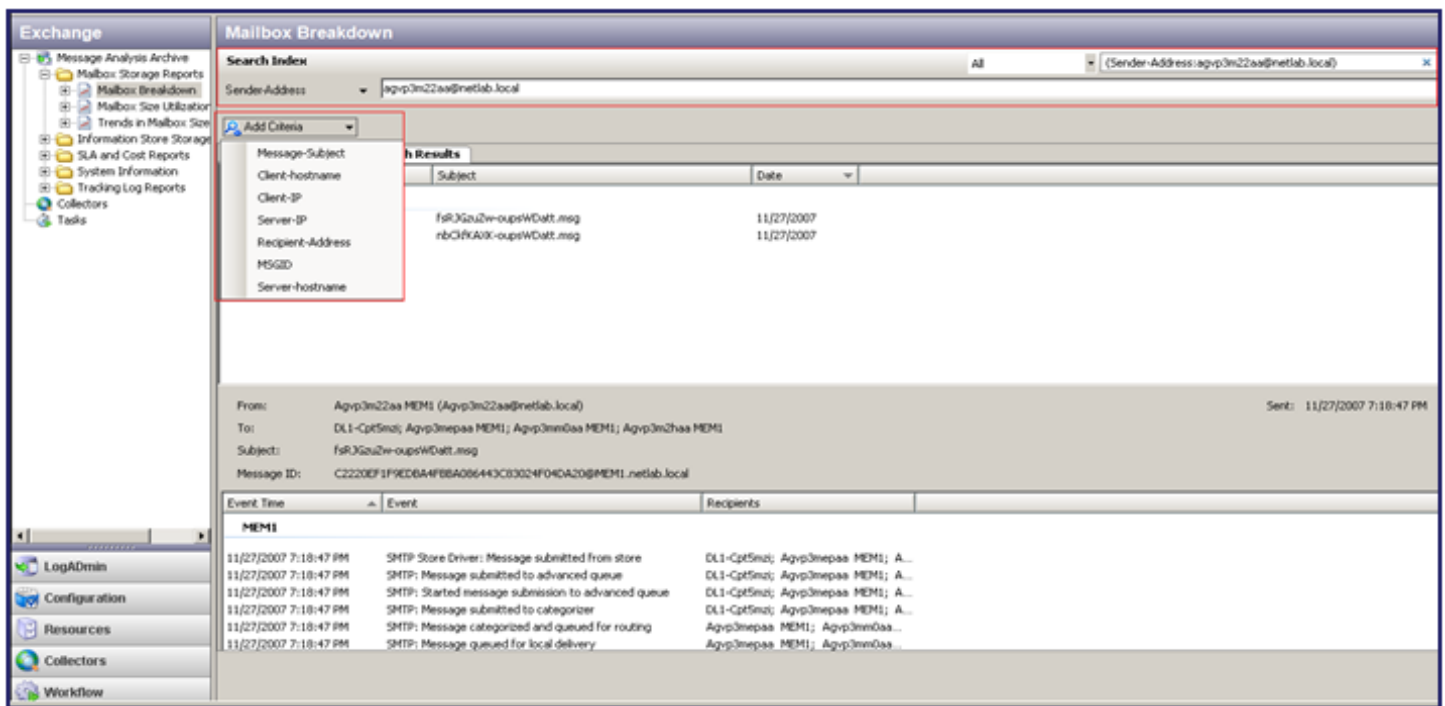


Figure 2

the flow of a message from server to server within the organization because all the tracking results came back to a single database and were correlated for me. The NetControl user interface is straightforward and intuitive, so using this over time shouldn't be a problem of any kind.

I wasn't able to directly evaluate maintenance because I was already using the current version of the software. However, the documentation indicates that installing a new version simply requires installation to the central Console. It handles the task of pushing updated agent software to those servers that require it.

Enterprise Practicality

I can see a couple of major and immediate uses that will benefit larger organizations. The message searching, as indicated earlier, is a must-have for organizations dealing with compliance (for example, checking to see whether critical information is leaving the company via email) as well as those who are dealing with, or may deal with, e-discovery as part of a legal proceeding. The chargeback reports are something I think most organizations should produce, if for no other reason than to understand how the overall messaging infrastructure is being utilized by different departments within the company. Message Analysis also includes a business intelligence component using Online Analytical Processing (OLAP) cubes, a feature I didn't test thoroughly, but which seems to provide much more advanced trending capabilities that I can see being extremely useful in larger companies. ♦

Windows Vista Remote Server Administration Tools

by Laura E. Hunter

After many months of waiting, the Remote Server Administration Tools (RSAT) for Windows Vista have finally shipped. A number of IT admins, both those who were early Windows Vista adopters and those who have adopted more of a “wait-and-see” attitude, have been waiting rather impatiently for this update to arrive.

Early adopters of Vista were almost universally frustrated by the lack of Windows Server administrative tools built-in to Vista. Unlike Windows 2000 and Windows XP, administrative tools for Windows server were not available with Windows Vista. Some administrators found a certain amount of success in installing the Windows Server 2003 Administrative Tools (adminpak.msi) on a Vista machine by using the workaround found in MS KB article 930056. Unfortunately, the workaround presented in this article was not a 100% fix, and was also not universally successful. Some of the Microsoft Management Console (MMC) snap-ins were still non-functional even with the workaround in place.

Now that Vista SP1 is here, Microsoft has released this new suite of tools as an out-of-band download from the Microsoft Web site, available from Microsoft KB Article 941314. The downloadable file itself is roughly 18MB in size, and is currently downloading with a filename of Windows6.0-KB941314-x86.msu. The MSU file extension is new to Windows Vista and Windows Server 2008, and refers to Windows Update packages that are available from the Windows Update Catalog or from <http://support.microsoft.com>.

RSAT can be installed interactively on individual Vista workstations as needed, but unfortunately, the installation process cannot currently be automated via a Windows Server Update Services (WSUS) server. As a workaround for this, Windows Vista includes the wusa.exe utility, which allows you to install .MSU files from the command line. This utility allows you to push a large-scale installation of RSAT using login scripts or other automation tools.

The RSAT download includes the following available tools; you can install an individual tool, a subset of the available tools, or the entire suite:

- ▶ Active Directory Certificate Services Tools
- ▶ Active Directory Domain Services (AD DS) Tools
- ▶ Active Directory Lightweight Directory Services (AD LDS) Tools
- ▶ BitLocker Drive Encryption Tools
- ▶ DHCP Server Tools
- ▶ DNS Server Tools
- ▶ Failover Clustering Tools
- ▶ File Services Tools
- ▶ Group Policy Management Tools
- ▶ Network Load Balancing Tools
- ▶ Network Policy and Access Services Tools
- ▶ SMTP Server Tools
- ▶ Storage Manager for SANs Tools
- ▶ Terminal Services Tools
- ▶ Universal Description, Discovery, and Integration (UDDI) Services Tools
- ▶ Windows System Resource Manager Tools

All these tools can be used to administer Windows Server 2008 networks, whether you’re working with an Active Directory (AD) domain or need to administer individual 2008 servers. A subset of the RSAT tools can also be used to administer Windows Server 2003 networks—the exception being tools pertaining to services such as the Network Policy and Access server role that is specific only to Windows Server 2008. The RSAT tools that are supported for use on Windows Server 2003 networks are as follows:

- ▶ All of the AD and Group Policy administration tools can target a 2003 domain controller: ADUC, AD Domains & Trusts, AD Sites & Services, the Group Policy Management Console
- ▶ Active Directory Certificate Services (this was the “Certification Authority” snap-in on 2003 servers)
- ▶ DNS
- ▶ DHCP
- ▶ Network Load Balancing
- ▶ Terminal Services tools
- ▶ UDDI

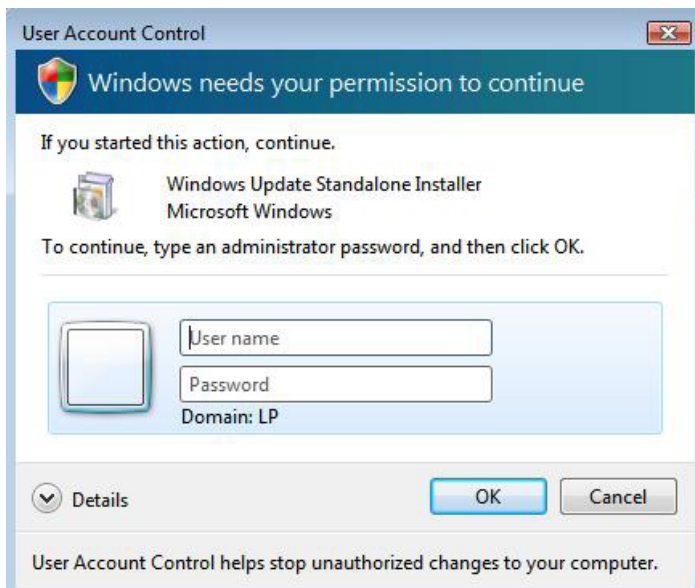


Figure 1: Prompting for administrative credentials before launching RSAT.

Similar to other built-in Vista tools and updates, RSAT adheres to the “Least User Access” model provided by User Access Control. So, logged onto a Vista machine as a non-administrative user, launching the RSAT installer displays a UAC over-the-shoulder elevation prompt (see Figure 1). Upon providing the username and password for an administrative user, the installation of RSAT itself is uneventful.

Once RSAT has been installed, you might be initially surprised at the lack of tools that appear in the Administrative Tools folder by default. Unlike the previous versions of adminpak.msi, simply installing RSAT does not make the new administrative tools available; you will need to take additional steps before you will be able to activate and use these features.

In another step towards increased security on the part of the new Microsoft client OS, the RSAT installer enables the RSAT tools to be added as a Windows Vista feature, but it does not actually install the binaries until they are specifically added via the control panel. This gives you the option to push RSAT to your desktops en masse to be used by your desk-side support staff.

To actually install the RSAT binaries, navigate to Start | Control Panel | Programs and Features | Turn Windows features on or off. If you are logged on as a non-administrative user when you take these steps, you will again be prompted for administrative credentials to add the RSAT binaries to your Vista installation.

Once you’ve installed the tools, you’ll notice that a number of them are largely unchanged in terms of functionality. Their user interfaces (UIs) have been made prettier and more “Vista-fied.” This includes the Terminal

Server tools such as Remote Desktops and Terminal Services Manager as well as the DHCP snap-in. File Server Resource Manager (FSRM) and Print Manager are largely the same interfaces that you would see on Windows Server 2003 R2 with the updated file/print functionality included.

In addition to the updated look-and-feel, another much-desired benefit is in the “Run as administrator” functionality. This feature within the right-click context menu works when you are logged on interactively as a non-administrative user and is helpful for elevating credentials on a one-time basis.

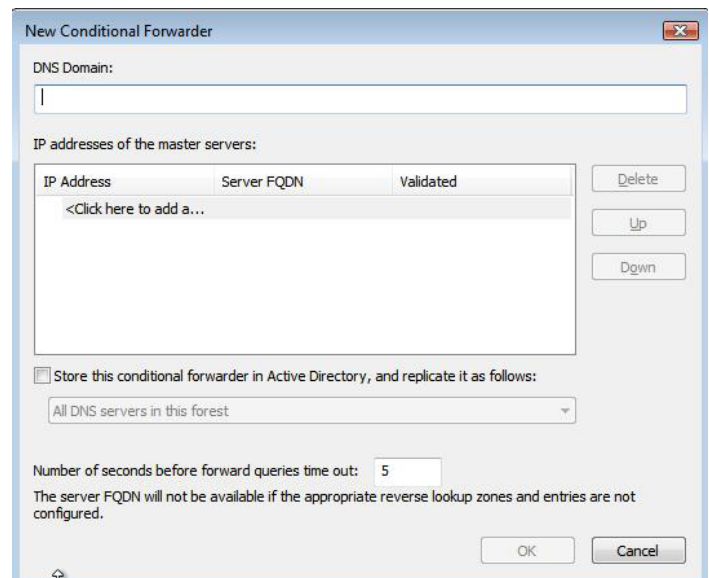


Figure 2: The Conditional Forwarder UI in the DNS MMC.

The DNS MMC is also largely unchanged; the major difference being the Conditional Forwarders UI (see Figure 2). As you can see from the Store this conditional forwarder in Active Directory, and replicate as follows check box, Windows Server 2008 AD now gives you the ability to store conditional forwarder information within AD rather than restricting it to a server-by-server configuration item.

Moving on to the AD tools, you’ll find little that has functionally changed in Active Directory Domains & Trusts, AD Sites & Services, and ADSI Edit. One change that many administrators will like is that ADSI Edit is now installed as part of the default administrative tools rather than requiring a separate installation from the Support Tools.

Active Directory Users & Computers has a few small but quite welcome improvements. The first is the Attribute Editor tab (see Figure 3), which gives you a view of all attributes of a particular object similar to what you’re used to seeing in ADSI Edit. You can customize your view of these attributes using the following filters:

- ▶ Show only attributes that have values
- ▶ Show only attributes that can be written to.
- ▶ Show or hide mandatory attributes for the object
- ▶ Show or hide optional attributes for the object
- ▶ Show or hide constructed attributes for the object
- ▶ Show or hide backlinks for the object
- ▶ Show or hide System-only attributes for the object

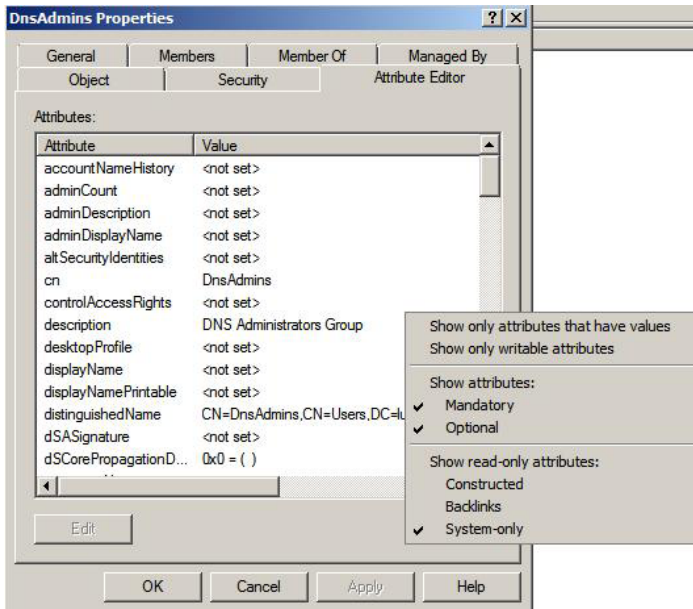


Figure 3: Using the new Attribute Editor tab to customize attributes via filters.

Specific to Windows Server 2008 AD, user objects in the new ADUC are displayed with a Password Replication tab, which indicates which Read-Only Domain Controllers (RODCs) have locally cached that user's password.

Finally, another administrative tool that has benefitted from some long-anticipated changes is the updated Group Policy Management console. This console now allows you to create and administer Group Policy Preferences, a new feature of Group Policy that ships with Windows Server 2008 and Vista and has been back-ported to Windows Server 2003 and Windows XP. As you can see in Figure 4, Group Policy preferences allows you far better control over numerous aspects of the UI, including pushing out drive mappings, printer connections, ODBC connections, files, shortcuts, and numerous additional configuration options. What may be most exciting about Group Policy Preferences is the fact that it does not require a Windows Server 2008 AD infrastructure. Group Policy Preferences can be deployed on Windows Server 2003 AD, so long as its Client-Side Extensions have been deployed as described in Microsoft KB article 943729.

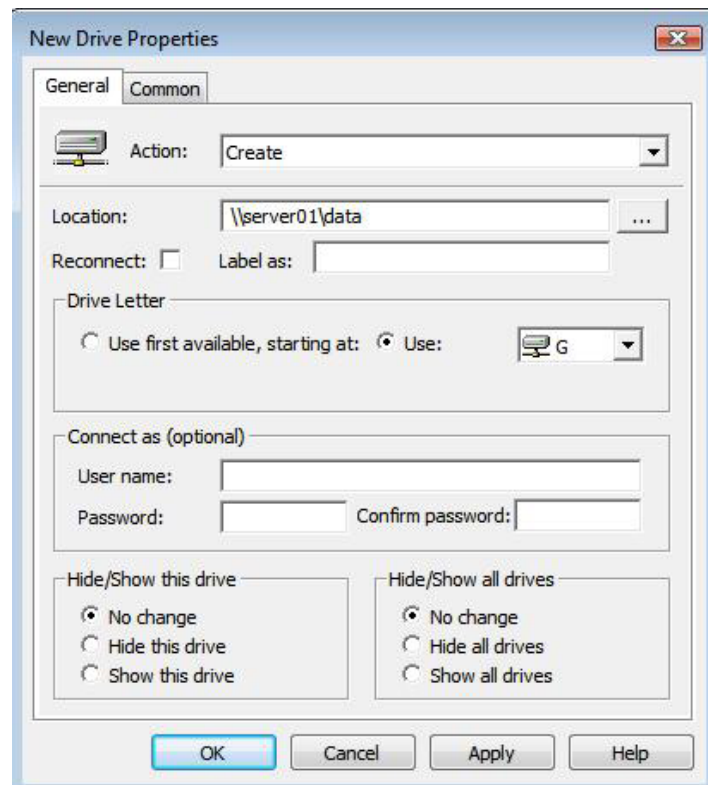


Figure 4: Group Policy preferences offers much control over numerous aspects of the UI.

All in all, the RSAT update for Windows Vista is an excellent addition to an administrator's toolset. One of the challenges faced by potential early adopters of Windows Vista was the fact that these administrative tools were not available. This fact left many with an unpalatable choice to continue running Windows XP solely for the availability of the administrative tools or to upgrade without the needed toolset support. With the introduction of RSAT, Windows administrators now have the ability to deploy a fully functional administrative workstation, with the potential to increase the adoption of Windows Vista in corporate IT departments. ♦

Laura E. Hunter (CISSP, MCSE: Security, MCDDBA, Microsoft MVP) is an Active Directory architect for a major engineering and staffing firm where she provides Active Directory planning, implementation, and troubleshooting services for business units and schools across an enterprise network. Laura is a four-time recipient of the prestigious Microsoft "Most Valuable Professional" award in the area of Windows Server-Networking. She is the author of the Active Directory Field Guide (APress Publishing) as well as co-author of the Active Directory Cookbook, Second Edition (O'Reilly).

The Deep Dive

Give Vista a Chance!

by Greg Shields

If you've been reading the Realtime Windows Server Community over the past month, you've been aware of my recent attempts to dispel the rumors about Windows Vista that have driven down its adoption rate. Many of those rumors are based on incorrect assumptions and a lack of time on the part of administrators to just simply check it out for themselves. Through my own digging, looking at the research of others, I've discovered that the source for much of this anti-Vista messaging is originating from the media itself.

This week's column is an adaptation of a post to the Community back on April 9th. In it, I give you a challenge to **Give Vista a Chance**. Vista has some excellent and compelling features that should drive its adoption, but only if we as administrators can grow accustomed to its new face—a process that takes time and effort. Read on to learn more...

Beware the Punditocracy

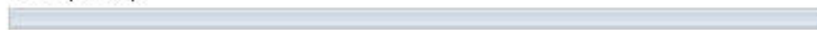
As I continue my campaign to dispel the Vista rumors in the world, I find further evidence of the media's role in pushing the "Vista sucks" meme. Now let me first say that administrators everywhere are a busy bunch. Actually taking the time for a thorough analysis of new technology to gain one's own opinion requires an amount of time that many administrators often don't have. But when established and respected media outlets such as ZDnet and InfoWorld continue to push this anti-Vista meme, I wonder if they realize the harm they're causing to the industry that is "systems administrators."

My reasoning for this commentary comes from an April 9th column written by Adrian Kingsley-Hughes, a renown blogger whom I read regularly and has lately taken to task what appears to be his own very subtle anti-Vista campaign. Through some careful title wording, the early April column suggests that everybody's throwing the baby out with the bathwater: *Who's Giving Vista a Miss and Waiting for Windows 7?*

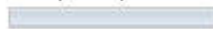
In his commentary, he takes a poll asking three questions of his readers. The first tells an interesting tale of the power of punditry. In this question we see how the recent "grass is greener" thinking affects the administrator population through the assumption that "Windows 7 has got to be better:"

If you've not already deployed Vista, does all this Windows 7 chatter make you want to hold out until 2010 and wait for the next version?

Yes (80%)



No (20%)




Total Votes: **2,902**


Continuing down this path, he suggests that continuing with Windows XP over the long haul—even in the case of reduced support options—is a better idea than making the jump. This concerns me particularly because a decision like this is more involved with risk-reduction in terms of support contract options than how one favors a particular OS:

If so, do you think that Windows XP is good enough to hold out until 2010?


Yes, I could stick with XP until 2010 with SP2 (51%)



Yes, but I'm eagerly awaiting SP3 (35%)



Not sure, 2010 is a long way away (14%)

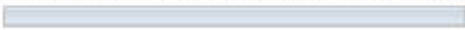


Total Votes: **2,889**

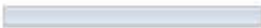
Lastly, we arrive at the kicker. His last question illuminates much of the problem with the Vista debate of today: Due to that inability to set aside the proper time, many people are choosing to believe the punditry over their own eyes. Though a goodly number of people (administrators or not) want to believe the “Vista sucks” meme, nearly the majority of them is sourcing their information not through their own opinions but of the opinions of others as well as voices in the media:

Based on what evidence are you giving Vista a miss?


I'm taking the word of others that it's not good enough (45%)



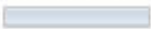
I tried it within the last few months and it didn't work well enough (25%)



I tried it soon after it was released and it didn't work well enough (17%)



I've tried it with SP1 RC/SP1 and it didn't work well enough (14%)



Total Votes: **2,520**

This last question tells the true sad tale about Vista’s relevance in today’s business networks. If we at the grassroots level can’t be bothered with taking the time to form our own opinions, Vista is doomed to wither on the vine. The punditocracy has been slighted by it and refuses to look back.

I get emails constantly from readers of both this community and my work with Redmond Magazine and MCPmag.com. Those readers tell me their joys and pains with Vista. The messages I get with positive feelings towards this OS reveal administrators who simply took the time to learn the new interface with all its quirks, changes, and newfangled widgets. The other half tell me stories of pain, but in most cases, also what appears to be a too-quick decision to drop it and run back to the comfort of what’s familiar. Nearly all the anti-Vista messages I get arrive full of incorrect assumptions and old data.

A Call to Action – Give Vista a Chance

As an old buddy of mine likes to say, **Give Vista a Chance**. Considering what I've discussed, I think we need to add to his comment, "...a rather extended one."

In fact, I challenge every Vista hater who reads my Realtime Windows Server Community as well as this newsletter to try the upgrade once again. But this time, give the new operating system three months.

That's the length of time you'll need to grow accustomed to where its icons have moved, where the "hidden" parts have been relocated, where your needed drivers are, and how to best manage it using the management tools and Group Policy. Microsoft has now released the Remote Systems Administration Tools (RSAT), a major omission and necessity for all Windows administrators. This release means that all the missing IT administration tasks formerly part of adminpak.msi are now fully available and supported in Vista.

If after three months, you still believe that "Vista sucks" and has no place in your IT environment, I'll concede defeat. But let me help you wade through some of the challenges. If, however, after three months, you begin to see the value of Vista in your environment, I want to hear about it.

So take on the **Realtime Give Vista a Chance Challenge**. Drop a comment here or email me at gshields@realtimepublishers.com. I respond to every message and we'll track your progress. ♦

Greg Shields, MCSE: Security, CCEA, is an independent author, speaker, and consultant, based in Denver, Colorado. With more than 10 years of experience in information technology, Greg has developed extensive experience in systems administration, engineering, and architecture. Greg is a contributing editor for both Redmond magazine and MCPmag.com, authoring two regular columns along with numerous feature articles, webcasts, and white papers. He is also the resident editor for Realtime Publishers' Windows Server Community at www.realtime-windowsserver.com. Greg is currently finishing his new book Windows 2008: What's New, What's Changed through SAPIEN Press.



SAPIEN
PRESS

Microsoft has released its next server operating system – Windows Server 2008 – and you need to know more about it. But you don't need the basics. You already know Windows 2003. You just need to know what's new and what's changed in Windows Server 2008. Read-Only Domain Controllers, the Group Policy Central Store, Terminal Server RemoteApps, Fine-Grained Password Policies. This quick and entertaining guide, written by Windows insider Greg Shields does just that. Focusing on the new technologies for installing, managing, and securing Windows Server 2008, you'll quickly ramp up your skills. Save yourself some time and money by skipping the basics and using your existing skills to master Microsoft's new server O/S.

Automate server installations * More effectively manage servers through Server Manager * Gain insight with Reliability and Performance Monitor * Implement powerful new Group Policy * Reduce your attack surface with Server Core * Complete better Active Directory backups * Deploy apps using Terminal Services * Secure your servers with the new Windows Firewall

TABLE OF CONTENTS	
Chapter 1: Introduction to Windows Server 2008	Chapter 7: Active Directory
Chapter 2: Installing Windows 2008	Chapter 8: Terminal Services
Chapter 3: Server Management	Chapter 9: Security & the Windows Firewall with Advanced Security
Chapter 4: Group Policy	Chapter 10: IIS 7.0
Chapter 5: Server Core	Chapter 11: Other New & Compelling Features
Chapter 6: Windows Server Virtualization	

http://www.sapienpress.com/Windows_Server_08.asp

Practical PowerShell

Local Account Management with PowerShell

by Jeffery Hicks

Last month, I gave you practical PowerShell tips on managing local account passwords for your member servers and desktops. Let's wrap up this topic with some additional functions for managing local user accounts.

You can download the code sample from the RealTimePublishers web site at http://www.realtime-windowsserver.com/code/vln5_Practical_PowerShell.zip

Get Local User Accounts

If you are the sole administrator, you likely know what local user accounts are established on your member servers and desktops. In case you don't or you'd like to perform a quick security audit to find the local accounts, the Get-LocalUsers function should get the job done (see Listing 1).

```
Function Get-LocalUsers {
    Param([string]$computer=$env:computername)

    $errorActionPreference="SilentlyContinue"

    [ADSI]$server="WinNT://$computer"

    if ($server.name) {

        $users=$server.psbases.children | where {
            $_.psbase.schemaclassname -eq "user"}

        $users | ForEach-Object {

            $obj=New-Object PSObject

            $obj | Add-Member -MemberType "NoteProperty" -Name "Computer" `
                -Value $computer.ToUpper()
            $obj | Add-Member -MemberType "NoteProperty" -Name "Name" `
                -Value $_.name.value
            $obj | Add-Member -MemberType "NoteProperty" -Name "FullName" `
                -Value $_.fullname.value
```

```

    $obj | Add-Member -MemberType "NoteProperty" -Name "Description" `
    -Value $_.Description.value

write $obj

}

} else {
    $msg="Failed to connect to "+$computer.ToUpper()
    Write-Warning $msg
}

}

```

Listing 1: The Get-LocalUsers function.

The function defaults to the local computername or you can specify a computername as a parameter. There is no provision for alternate credentials. You must launch this function with credentials that have administrative privileges on the remote computer or create a secure channel using alternate credentials using the NET USE command to map a drive to an administrative share on the remote computer.

Using ADSI, a connection is made to the server or desktop:

```
[adsi]$server="WinNT://$computer"
```

If no connection was established, the \$server.name property won't exist and the function will exit, writing a warning message:

```

} else {
    $msg="Failed to connect to "+$computer.ToUpper()
    Write-Warning $msg
}

```

Because of the way PowerShell adapts the WinNT provider, I need to access the underlying PSBase object and its children property. The server object is a parent object that contains users, services, printers, and groups as children. To filter out only user accounts, I'll check the schemaclassname for each object. If it is a user, I'll keep it:

```

$users=$server.psbases.children | where {
    $_.psbase.schemaclassname -eq "user"}

```

Each object will have properties like this:

```

UserFlags           : {66113}
AccountExpirationDate : {12/31/2009 1:00:00 AM}
MaxStorage          : {-1}
PasswordAge         : {6404002}

```

```

PasswordExpired      : {0}
LoginHours           : {255 255 255 255 255 255 255}
FullName             : {Tech}
Description           : {Help Desk Account}
BadPasswordAttempts  : {0}
HomeDirectory        : {}
LoginScript          : {}
Profile              : {}
HomeDirDrive         : {}
Parameters           : {}
PrimaryGroupID       : {513}
Name                 : {Tech}
MinPasswordLength    : {0}
MaxPasswordAge       : {3628800}
MinPasswordAge       : {0}
PasswordHistoryLength : {0}
AutoUnlockInterval   : {1800}
LockoutObservationInterval : {1800}
MaxBadPasswordsAllowed : {0}
objectSid            : {1 5 0 0 0 0 0 5 21 0 0 0 32}

```

However, I have found it easier to create a custom object for each user object by piping the collection of users to `ForEach-Object` and then, for each pipelined user object, create a `PSObject`:

```

$users | ForEach-Object {

$obj = New-Object PSObject

```

I'll add new members, or properties, to the object from some of the current user's properties and write the object to the pipeline:

```

$obj | Add-Member -MemberType "NoteProperty" -Name "Computer" `
-Value $computer.ToUpper()
$obj | Add-Member -MemberType "NoteProperty" -Name "Name" `
-Value $_.name.value
$obj | Add-Member -MemberType "NoteProperty" -Name "FullName" `
-Value $_.fullname.value
$obj | Add-Member -MemberType "NoteProperty" -Name "Description" `
-Value $_.Description.value

write $obj

```


Here's an example of the function in action:

```
PS C:\> get-localusers server01 | format-table -autosize
```

Computer	Name	FullName	Description
SERVER01	Administrator		Built-in account for admi...
SERVER01	ASmithee		Built-in account for gues...
SERVER01	greg	Greg Shields	DHCP admin
SERVER01	jeff	Jeff Hicks	local admin account

Have a list of computers you want to check? Here's an expression you could try:

```
PS C:\> get-content computers.txt | foreach {get-localusers $_} `
>> | tee-object localusers.txt
```

Each computer name in computers.txt is passed by the Get-Content cmdlet to the Get-LocalUsers function, and that output is piped to the Tee-Object cmdlet which displays the results to the console and saves them to the specified text file. Prefer to save the output to a CSV file? Easily done with this:

```
PS C:\> get-content computers.txt | foreach {get-localusers $_} `
>> | export-csv localusers.csv -notypeinformation
>>
```

WINDOWS POWERSHELL TRAINING

3 DAYS

ScriptingAnswers.com®
SPECIAL FORCES TRAINING

WHEN: AUGUST 4-6, 2008,
15 STUDENTS MAXIMUM

LOCATION: THE UNIVERSITY OF CHICAGO
GLEACHER CENTER, CHICAGO

ScriptingAnswers.com ONLINE TRAINING
Our all-new online training offers a hybrid approach similar to the Distance Learning programs offered by many community colleges and universities.

For more information: www.scriptingtraining.com

SAPIEN

Or perhaps you would like to find all the servers that might have a particular user:

```
PS C:\> get-content computers.txt | foreach {get-localusers $_} `
>> | where {$_.name -like "jeff"}
```

This expression will show me all the machines in computers.txt that have a local account that starts with “jeff.” PowerShell makes it very easy to learn new things about your network with a minimal amount of work.

Build a Password Report

We can combine this function with the Get-PasswordAge function from last month to create a password age report for all user accounts. Load both functions into your PowerShell session before you try these examples. Now you can run Get-LocalUsers and pipe the results to ForEach, executing Get-PasswordAge for each passed object. Here’s what it looks like when run on the local machine:

```
PS C:\> Get-LocalUsers | foreach {Get-PasswordAge -computer $_.computer -account $_.Name}
| format-table -auto
```

Computer	Account	PasswordAge	LastChanged
XPDESK01	ADMINISTRATOR	732	3/3/2006 10:23:54 PM
XPDESK01	ASMITHEE	0	3/4/2008 10:23:54 PM
XPDESK01	ASPNET	8	2/25/2008 10:23:55 PM
XPDESK01	HELPPASSISTANT	732	3/3/2006 10:23:55 PM
XPDESK01	SUPPORT_388945A0	732	3/3/2006 10:23:55 PM

Of course, you can easily specify a remote computer name. The output object of Get-LocalUsers contains a property for the computer name, which makes it pretty simple:

```
PS C:\> Get-LocalUsers -computer vista02 | foreach {
>> Get-PasswordAge -computer $_.computer -account $_.Name} `
>> | sort PasswordAge -Descending | Format-Table -auto
>>
```

Computer	Account	PasswordAge	LastChanged
VISTA02	HELPPASSISTANT	292	5/17/2007 10:31:23 PM
VISTA02	ADMINISTRATOR	292	5/17/2007 10:31:04 PM
VISTA02	SUPPORT_388945A0	292	5/17/2007 10:32:00 PM
VISTA02	JHICKS	177	9/9/2007 10:31:32 PM
VISTA02	LUCKY	162	9/24/2007 10:31:41 PM
VISTA02	LUSER	35	1/29/2008 10:31:50 PM
VISTA02	TECH	34	1/30/2008 10:32:09 PM
VISTA02	__VMWARE_USER__	6	2/27/2008 10:30:55 PM
VISTA02	GUEST	0	3/4/2008 10:31:13 PM

These examples only looked at the user accounts on a single computer, but I could just as easily parse a list of computer names with an expression like this:

```
"server1","server2","server3" | foreach {  
    get-localusers $_ | foreach {  
        get-passwordage -computer $_.computer -account $_.name  
    }  
}  
| sort Computer | format-table -autosize
```

A Domain Controller Is Also “Local”

One last comment before we leave this topic: The WinNT provider is not limited to member servers or desktops. You can connect to an Active Directory (AD) domain controller and access the directory service as a flat namespace. The WinNT provider doesn't understand things like organizational units (OUs) but it does recognize user accounts. Here is a PowerShell expression that will get all accounts from your domain and display the results sorted by PasswordAge in descending order:

```
get-localusers $env:userdomain | foreach {  
    get-passwordage -computer $_.computer -account $_.name  
} | sort PasswordAge -descending | format-table
```

You can either specify the name of a domain controller or the domain name itself, as I've done here using the %userdomain% environmental variable. Depending on the number of user objects in your domain, this may take a while to run, especially remotely.

That's all I have time for this month, but stay tuned. I have one more password-related function you might appreciate. In the meantime, keep the PowerShell pipeline flowing! 💎

Jeffery Hicks, MCSE, MCSA, MCT, and Microsoft PowerShell MVP, is a Scripting Guru for SAPIEN Technologies. Jeff is a 16-year IT veteran. He has co-authored and authored several books, courseware, and training videos on administrative scripting and automation. His latest book is WSH and VBScript Core: TFM (SAPIEN Press 2007). You can contact him at jhicks@sapien.com.

Exclusively Exchange

Moving to Exchange 2007 with a Little Help

by J. Peter Bruzzese

With each release of Exchange comes changes in the messaging structure and architecture that make the upgrade path a labyrinth of decisions. This time, that maze is slightly different due to concepts like *no in-place upgrades, migrations, transition, and co-existence*.

Last month's column explored the 'free' method of moving toward Exchange 2007 from Exchange 2000/2003 with Microsoft tools. But that may not be your particular focus. What if you need to migrate from Exchange 5.5 or GroupWise or Domino? What if you have an IMAP mail server?

Exchange 2003 had the Exchange Migration Wizard to take you from Domino, GroupWise or IMAP to 2003. Well, aside from Domino (which has the Microsoft Transporter Suite), Exchange 2007 is lacking in terms of cross-platform migration tools. So you might consider making

the move to Exchange 2003 first and then transitioning over to Exchange 2007, as we previously discussed. But you must be wondering "Is there a better method out there? An option that doesn't require using Exchange 2003 as your intermediate step in the process." This month's column highlights third-party solutions that can help make your life a bit easier... at a cost.

The Tools, the Price

Without doing a full review (thumbs up/thumbs down) on different products, let's consider a few of the outstanding players in the market for Exchange migrations and transitions.

Quest Software: Migration Suite for Exchange

Even Microsoft states that if you are migrating to Exchange 2007 from

Exchange 5.5/2000/2003, GroupWise, or Notes, Quest migration solutions include everything you need for the successful migration of your messaging environment. The obvious benefit of this option is the ability to move directly from an Exchange 5.5 (or mixed) organization to Exchange 2007 and do so with a 'coexistence through synchronization' that has no impact on resources or users.

For more information about Quest solutions, see http://www.quest.com/exchange_2007/. Also, before performing a migration, check out the very interesting article "Saving Time and Money by Archiving Before a Migration" by Ron Robbins and Peter terSteege at <http://www.quest.com/documents/list.aspx?contenttypeid=22&searchoff=true&technology=&prod=133&prodfamily=&loc>.

Priasoft: Migration Suite for Exchange

With the Priasoft Migration Suite for Exchange, you can migrate from Exchange 5.5, 2000, or 2003 over to 2007. Several tools in the suite can assist in finding hidden problems lurking in the background of a migration:

- ▶ Migration Assessor for Exchange
- ▶ Public Folder Analyzer, which

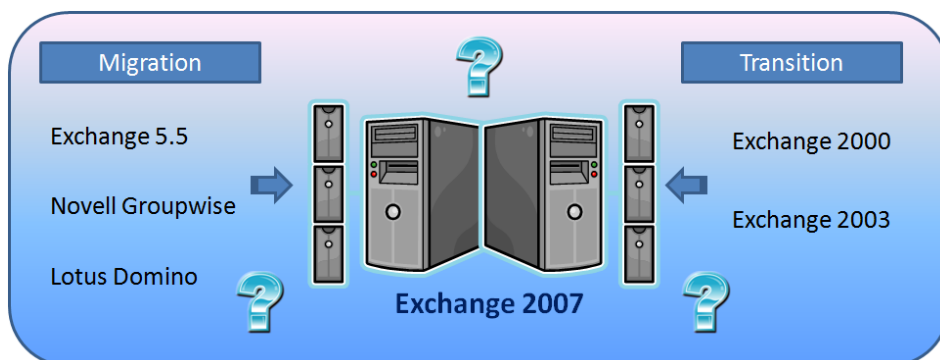


Figure 1: The many decisions involved in the move to Exchange 2007.

supports folder and permissions migration of public folder stores

- Mailbox Analyzer, which provides summary reports for migration planning

With the promise of 'no disruption to end users before, during, or after the migration,' you might want to learn more about Priasoft migration tools at <http://www.priasoft.com/exchangemigration/products.asp>.

NetPro: NetMigrate 5.2 for Exchange

A simple, wizard-like interface walks you through the process of moving from one Exchange environment (5.5/2000/2003) to 2007. One of the useful features included is a tool called NetPro Migration Services that help you clean up your organization before the move so that you minimize the risks associated with migration (yes, there is always risk). Another cool option is the roll-back feature that lets you reverse changes at any time.

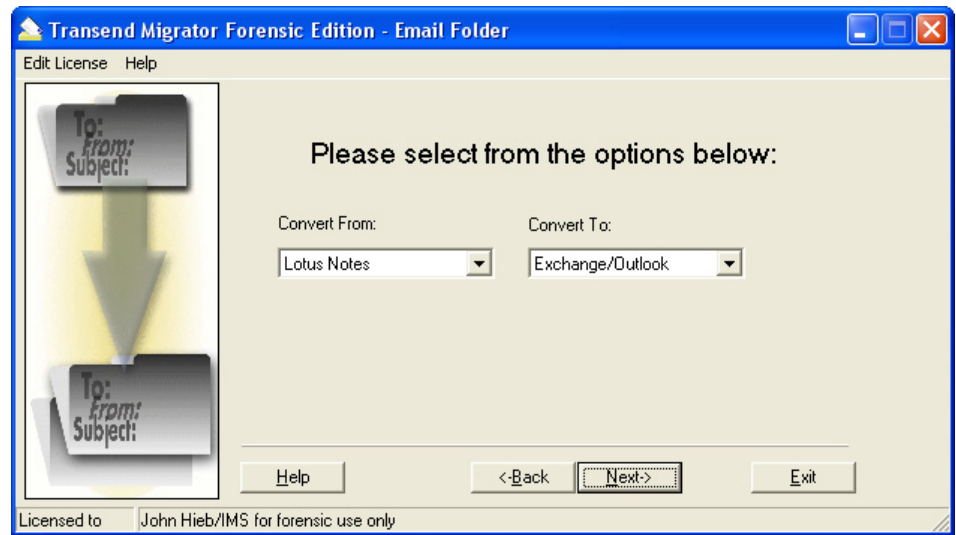


Figure 2: The Transend Migrator wizard interface.

Learn more about NetPro's NetMigrate at <http://www.netpro.com/products/netmigrate-for-exchange/index.cfm#>.

Transend: Migrator 7.0

This mailbox migration solution is worth considering for converting email data from both email systems and clients. Thus, if you are moving from GroupWise or an IMAP mail

server, rather than set up Exchange 2003 and move first over to 2003 and then to 2007, you might consider a direct move with Transend Migrator. In addition, client mailbox conversion is provided for Netscape/Mozilla/Thunderbird, Eudora, Pegasus, AOL, Outlook Express, and a host of others. For a full list of supported email conversions, go to http://www.transend.com/supported_mail_systems.asp.


CLIPTRAINING.COM



We offer the following services:

- An online training library that you can subscribe to monthly or yearly
- Customized training clips to help alleviate your chronic help desk challenges
- A ClipTraining Appliance (CTA, pronounced CheeTAh) that plugs right into your organization, providing instant training and support to your users through web services



Meet J. Peter Bruzzese:

Co-Founder of ClipTraining, Director of Technical Training, Screencasting Producer



Over the past 15 years, Peter has worked with Goldman Sachs, CommVault Systems, and Microsoft, to name a few. He holds the following certifications: from Microsoft, MCSA 2000/2003, MCSE NT/2000/2003, and MCT with MODL; from Novell, CNA; from Cisco, CCNA; from CIW, CIW Master and CIW Certified Instructor; from CompTia, A+, Network+, and iNET+. Most recently, Peter has become a Microsoft Certified IT Professional: Enterprise Messaging Administrator (MCITP: Enterprise Messaging Administrator).



Buy the latest book from Peter "Tricks of the Vista Masters" on Amazon.com

Although we've been discussing third-party solutions for migration, you might consider an archiving solution as well. For example, tools such as CommVault's Archive for Exchange that can archive Exchange 5.5 content and restore to Exchange 2007. Although this method is not the focus of this particular article, it's always good to consider all angles and keep your options open for new possibilities.

Sharpening Tools

Confucius said "The expectations of life depend upon diligence; the mechanic that would perfect his work must first sharpen his tools." Application here? Before deciding on the tool you need to perform a transition, make sure you consider different options and analyze the cost to ensure success. Then choose the right tool and make sure you know fully how to use it before proceeding diligently with your transition or migration to Exchange 2007. ♦

J. Peter Bruzzese is an MCSE (NT,2K,2K3)/MCT, and MCITP: Enterprise Messaging Administrator. His expertise is in messaging through Exchange and Outlook. J.P.B. is the Series Instructor for Exchange 2007 for CBT Nuggets. His latest book is "Tricks of the Vista Masters". He is co-founder of ClipTraining.com, a provider of short, educational screencasts on Exchange, Windows Server, Vista and Office 2007. You can reach Peter at jpb@cliptraining.com.

Copyright Statement

© 2008 Realtime Publishers, all rights reserved. This eJournal contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers (the "Materials") and this work and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers or its sponsors. In no event shall Realtime Publishers or its sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com. ♦