Specops Software presents:

THE
POWER
OF GROUP
POLICY

By Danielle Ruest and Nelson Ruest

The Power of Group Policy

Rely on Active Directory's Group Policy to control change in your network from A to Z.

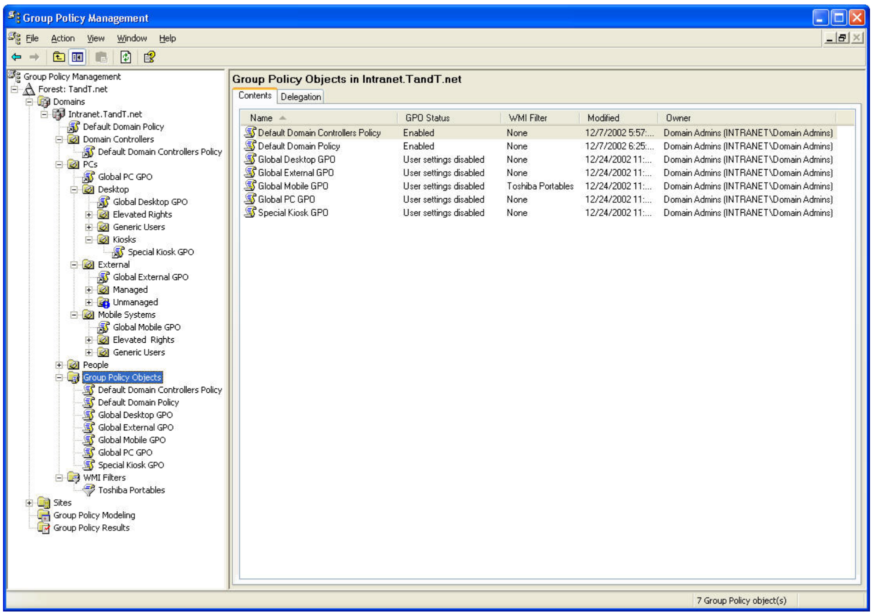
Active Directory (AD) is by far the best feature that Microsoft ever built into Windows. It's hard to imagine that some administrators are still struggling on with Windows NT today when it is so simple to move to Windows Server 2003 (WS03) and implement Active Directory (see Resources). But what's even more powerful than just AD is its ability to manage objects through Group Policy. Group Policy Objects (GPO) let you manage five elements of Windows systems:

- **User and Computer Settings** — Windows Server 2003 includes Administrative templates that allow GPOs to write specific settings to user (HKEY_CURRENT_USER) and computer (HKEY_LOCAL_MACHINE) registry hives.
- **Scripts** — Windows 2000, XP and WS03 can run Startup and shutdown scripts as well as logon and logoff scripts.
- **Data Management** — With Folder Redirection, WS03 can redirect user folders from the desktop to a central server location allowing full availability of these folders from any PC as well as centralized backup of user information. This feature is completely transparent to users. All they do is continue to work with the My Documents folder which is cached locally for faster availability.
- **Software Lifecycles** — Windows Server 2003 can Deploy software to both desktops and servers. Ideally, software products will be integrated with the Windows Installer service. WS03 can also automatically remove software from client systems.
- **Security Settings** — WS03 can Centrally manage security settings for PCs, servers and users through GPOs. You can also restrict access to software applications through Software Restriction Policies—policies which control which software is allowed to run in your network.

With Windows Vista, Microsoft is taking Group Policy to another level, adding almost 800 new settings bringing the total number of settings controllable through GPOs to 2,450. That's a lot of settings. In addition, Vista will support multiple Local Security Policies, letting you design different security settings for different user types. With Windows Server Codenamed 'Longhorn', Microsoft will invest even more into Group Policy.

The Inner Workings of GPOs

Group Policy provides one single interface for systems management through Microsoft's Group Policy Management Console or GPMC (see Figure 1). The GPMC provides a central location for the control of all settings. Of course, since GPOs are applied in a specific order, you need to marry your GPO strategy with the structure of your AD. When GPOs are applied, computer settings are applied first, and then the system applies user settings. It makes sense since the computer system boots up before the user can log in.



Group Policy Objects in Intranet.TandT.net

Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	12/7/2002 5:57:...	Domain Admins (INTRANET\Domain Admins)
Default Domain Policy	Enabled	None	12/7/2002 6:25:...	Domain Admins (INTRANET\Domain Admins)
Global Desktop GPO	User settings disabled	None	12/24/2002 11:...	Domain Admins (INTRANET\Domain Admins)
Global External GPO	User settings disabled	None	12/24/2002 11:...	Domain Admins (INTRANET\Domain Admins)
Global Mobile GPO	User settings disabled	Toshiba Portables	12/24/2002 11:...	Domain Admins (INTRANET\Domain Admins)
Global PC GPO	User settings disabled	None	12/24/2002 11:...	Domain Admins (INTRANET\Domain Admins)
Special Kiosk GPO	User settings disabled	None	12/24/2002 11:...	Domain Admins (INTRANET\Domain Admins)

7 Group Policy object(s)

Figure 1: The Group Policy Management Console

In addition, local and central GPOs have a specific application order:

1. The local GPO is applied at computer startup.
2. If available, site GPOs are applied next.
3. Domain GPOs are applied after site GPOs.
4. Organizational unit GPOs are applied last. If the object (either computer or user) is located within a child OU and the child OU contains an additional GPO, this GPO is applied last.

This process is often called the **L-S-D-OU** process for Local-Site-Domain-OU application order (see Figure 2). If there are conflicts between policies, the last policy provides the applied setting. For example, if you deny access to an item in the Start Menu in the domain policy, but it is allowed in an OU policy, the final result will be that access will be allowed.

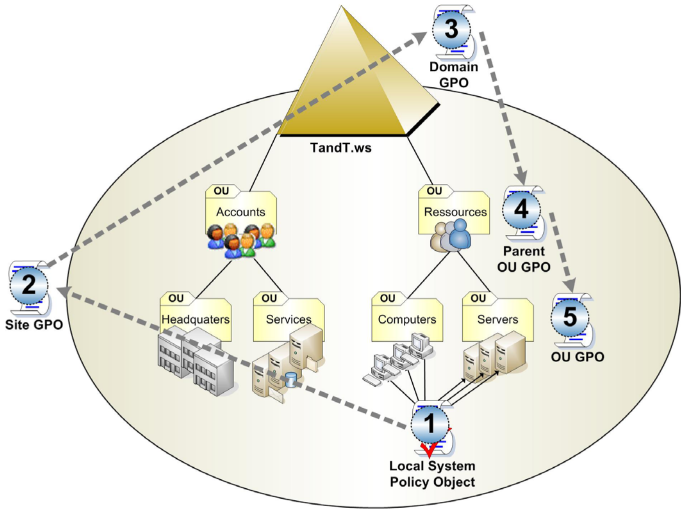


Figure 2: The GPO Application Order

The organizational unit structure of your AD has a direct impact on how GPOs are applied. The final result of GPO application is called the **resultant set of policies** (RSoP). Windows Server 2003 includes an RSoP tool that allows you to debug policy application so that you can identify the result of multiple policy application on a specific object.

Policy application begins as soon as the computer is powered on. It uses a 10-step process (see Figure 3):

1. At startup, the computer sends a DNS query to locate the closest DC.
2. Once the DC is identified, the computer creates a secure link to that DC.
3. The computer pings the DC to identify if it is on a slow link. If the answer is yes, only critical GPO settings will be applied.
4. The computer connects to AD through the lightweight directory access protocol (LDAP).
5. It queries AD to find out all of the GPOs linked to its OU and parent OUs.
6. It queries AD to find out all of the GPOs linked to its domain.
7. It queries AD to find out all of the GPOs linked to its site.
8. Once it has the list of GPO names, it queries the Group Policy Container (GPC) to identify the path to each of the Group Policy Templates (GPT) it must apply. The GPTs are located in the Domain Controller’s Sysvol share.
9. The computer reads the GPT.INI file located in the GPT folder for each GPO it must apply. This file lists the GPT’s current version number, a number that is incremented every time you make a change to the GPO. By default, This number change forces objects to reapply the GPO because some settings have changed. If the number is the same as it was the last time it was applied, the object does not reapply the GPO. Of course, this behavior can be changed through a Group Policy setting.

10. If the GPT's version number has changed, or if the GPO is set to always refresh, the computer's client-side extensions—the components that are used to apply GPOs—process all of the applicable GPOs. Afterwards, all applicable startup scripts are run. Since these scripts are run without a user interface, they are set to run for a maximum amount of time—600 seconds by default—in case the script hangs while running.

Once this process is complete, the computer will allow logons and display the logon splash. Everything except steps 1 to 3 is reapplied when a user logs on. Steps 4 to 10 are exactly the same unless GPO Loopback is enabled. Loopback can replace computer settings with the user's or replace the user's settings with the computer settings.

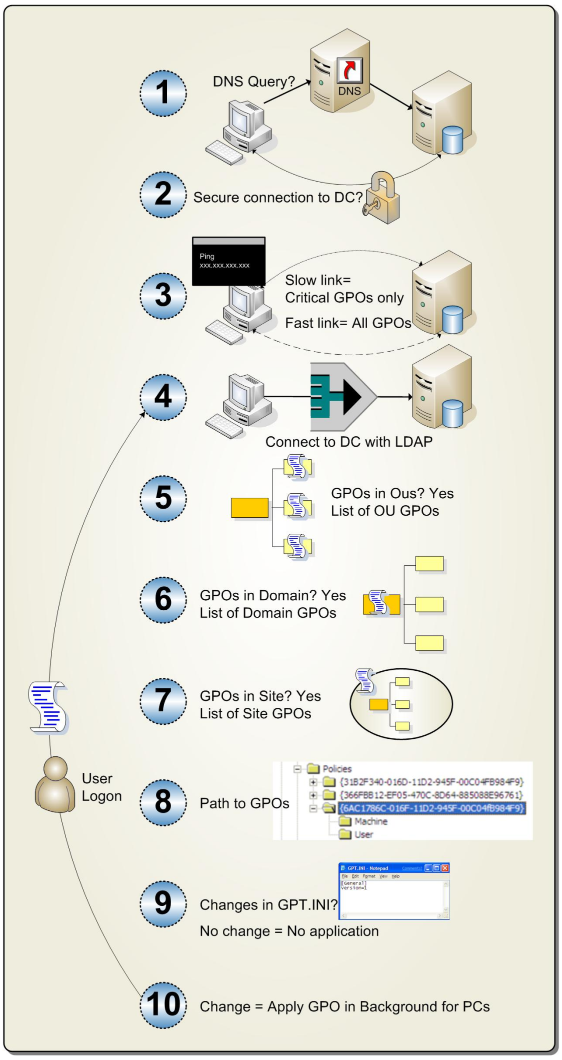


Figure 3: Computer and User GPO Application Process

Windows XP and Vista use asynchronous policy application while Windows Server 2003 and Windows 2000 use synchronous processing. This means that For servers and Windows 2000 systems, the computer session won't open until the entire list of GPOs are processed including any scripts that are referenced in the GPO. On Windows XP and Vista, GPO processing is delayed to speed up the session opening process. This is called Fast Logon Optimization. This is part of Microsoft's efforts to have client systems launch faster.

The Ideal Tool for Systems Management

There is a lot more to Group Policy, but this covers at least the basics of GPO application. As you can see, working with GPOs is really the very best way to manage Windows systems linked to an Active Directory. Why? Because once a policy is set, you don't have to do anything else. That's management simplicity. How many tools can you rely on to just work at all times?

Given the power of Group Policy, you'd think Microsoft would have done more to make it the very best management tool on the market, especially for Windows systems management. But, right now, there are still failings in their GPO strategy. For example, if you want to inventory your systems, you have to use a different tool. That's a bit odd since AD already contains information about every single computer system in your network—remember those computer accounts? Also, when deploying software through AD, you'll find that despite the fact that it works well, there is no way to tell whether a software deployment actually occurred—except, of course, if you actually connect to the PC you were deploying the software to and verify that it is installed. That's because AD does not include any software deployment reporting features. Another aspect that is lacking is bandwidth control. if you deploy Microsoft Office Professional 2007 to your PCs, you'll find that you can't control how much bandwidth it takes and you can't control when the deployment begins. Your best bet is to start the deployment at night and hope it doesn't kill your network.

It seems unfortunate that you would have to go through the entire process of designing and deploying your Active Directory, including domains, sites, organizational units, groups, service accounts and so on, and then when you're ready to take advantage of this design, you find you need to perform another deployment just to implement a systems management tool. It is odd, but right now, with Microsoft's default AD tools, that is what you need to do.

Fortunately, there is help. Specops Software offers some very powerful add-ons to Active Directory that take Group Policy to the next level. In fact, Specops has three offerings that can really help:

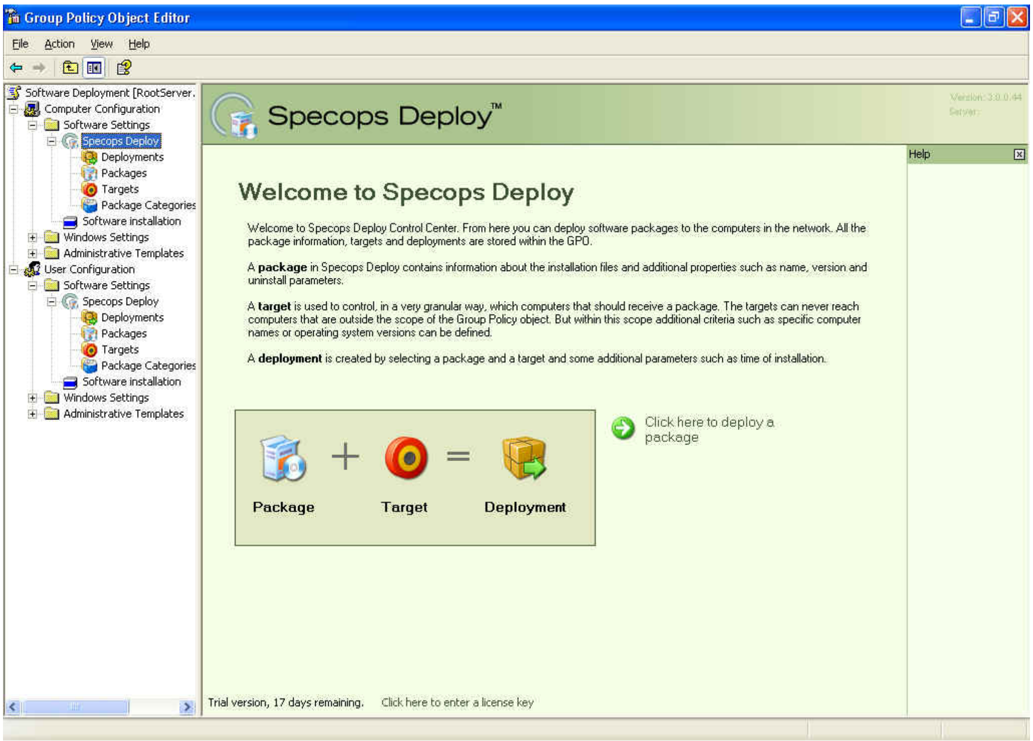
- **Specops Deploy** — an add-on that puts AD software deployment on steroids.
- **Specops Inventory** — an add-on that relies on AD to perform both hardware and software inventories.
- **Specops Gpupdate** — a free tool that you can deploy to client systems to gain more control over them.

These three tools can really make a difference. Each interacts with systems through extensions of the GPMC, keeping all management activities within a familiar interface for system administrators. In addition, both Inventory and Deploy offer stand-alone Web-based console that make it much easier to delegate administrative activities since you don't need to deploy anything to deliver this delegation. Just point your administrators to the Web link, configure their security access in AD, and off you go.

There is a lot to gain from working with Specops tools. First, you get to reuse your AD architecture to its fullest without having to perform another complete systems management tool deployment. Of course, Specops Deploy and Inventory require additional components—a database for example, to store all inventory and deployment information. Deploy also requires MS Message Queuing service (MSMQ) as well as a distribution point for software delivery. The latter, distribution points, can simply be any file share server on your network. If you want to get really smart, then use WS03 R2 and rely on the newly improved Distributed File System Replication Service (DFSRS), which will perform delta replications from one file share to any number of other shares. This gains you automatic bandwidth control for the distribution points. Then you can perform deployments locally to any system in any site. Even then, Deploy will rely on the Background Intelligent Transfer Service (BITS)—the same system used by Microsoft Update—to control bandwidth from the client to the distribution point.

Inventory only needs an external database. Since the AD database is hierarchical, you don't want it storing inventory information, or any information which is subject to change frequently. That's why you should implement a proper SQL Server database. either versions of SQL Server, 2000 or 2005, will work, though you should really rely on the latest edition since it is so much more secure.

As you can see, deploying both of these tools is relatively simple compared to everything else on the market. And once they are up and running, you'll find that no training is required since both rely on the familiar interfaces of Group Policy (see Figures 4 and 5). Then, you can use Inventory to find out if your systems are ready for Vista, or just to finally find out what you have out there. You can also rely on these tools to deploy the new version of Microsoft Office Professional 2007. Better yet, you can rely on them to perform your Vista deployment. Perform all inventories with Inventory, use Microsoft's new Vista deployment tools—WIM image format, ImageX, Computer System Image Manager, Windows Deployment Services, User State Migration Tool—to perform the OS deployment, and rely on Deploy to perform all software deployment once the image is in place. You can even use Deploy to create the reference computer and expect that all software installations are fully manageable once the image is deployed. That's simple deployment.



Welcome to Specops Deploy

Welcome to Specops Deploy Control Center. From here you can deploy software packages to the computers in the network. All the package information, targets and deployments are stored within the GPO.

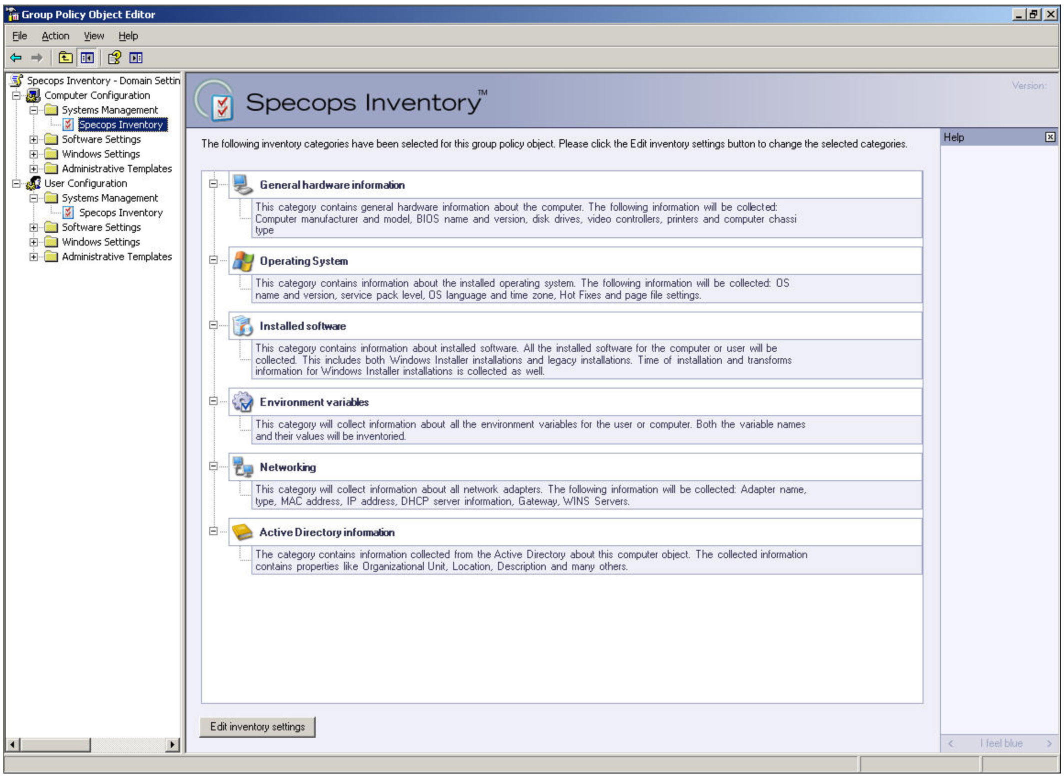
A **package** in Specops Deploy contains information about the installation files and additional properties such as name, version and uninstall parameters.

A **target** is used to control, in a very granular way, which computers that should receive a package. The targets can never reach computers that are outside the scope of the Group Policy object. But within this scope additional criteria such as specific computer names or operating system versions can be defined.

A **deployment** is created by selecting a package and a target and some additional parameters such as time of installation.

Trial version, 17 days remaining. Click here to enter a license key

Figure 4: Specops Deploy provides a simple interface for software deployment



The following inventory categories have been selected for this group policy object. Please click the Edit inventory settings button to change the selected categories.

General hardware information

This category contains general hardware information about the computer. The following information will be collected: Computer manufacturer and model, BIOS name and version, disk drives, video controllers, printers and computer chassi type

Operating System

This category contains information about the installed operating system. The following information will be collected: OS name and version, service pack level, OS language and time zone, Hot Fixes and page file settings.

Installed software

This category contains information about installed software. All the installed software for the computer or user will be collected. This includes both Windows Installer installations and legacy installations. Time of installation and transforms information for Windows Installer installations is collected as well.

Environment variables

This category will collect information about all the environment variables for the user or computer. Both the variable names and their values will be inventoried.

Networking

This category will collect information about all network adapters. The following information will be collected: Adapter name, type, MAC address, IP address, DHCP server information, Gateway, WINS Servers.

Active Directory information

The category contains information collected from the Active Directory about this computer object. The collected information contains properties like Organizational Unit, Location, Description and many others.

Figure 5: Specops Inventory offers several inventory categories

But the icing on the cake is Specops free Gpupdate tool. This small Windows Installer file can be installed on each system through Specops Deploy and once it is in place, It will give you many additional controls over any computer system in Active Directory. Use AD Users & Computers, another familiar tool to remotely shutdown or restart any computer. Gpupdate also gives you access to Wake-On-LAN (WOL) so that you can remotely launch any computer that may not already be turned on (see Figure 6). What's even better is that Gpupdate will give you complete graphical reports on the status of all your systems. Now that's pretty cool. What's even better is that since its free, you can take advantage of it right now.

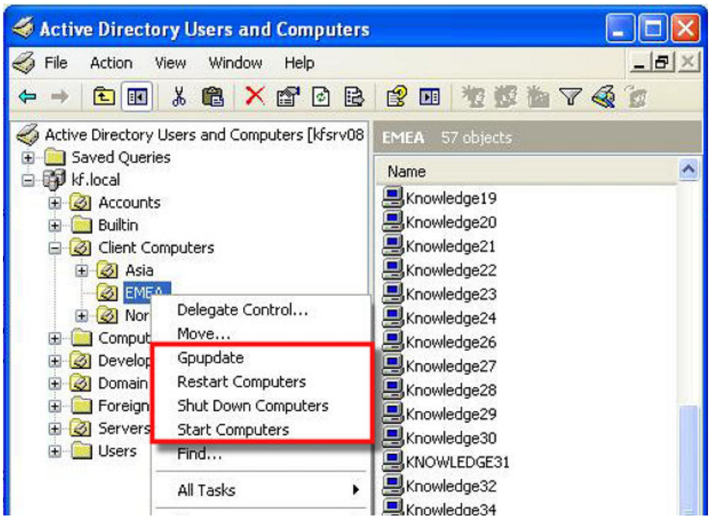


Figure 6: Specops Gpupdate gives you control over any computer in AD

Your Next Step

If you want to make the most of your investment in Active Directory, take a close look at Specops software offerings. They are common sense tools that build on existing technologies without reinventing the wheel to provide full functionality—the functionality that every system administrator expects—without the need for retraining. Microsoft has made AD its most powerful tool. Specops turns it into what it should be: the center of your Windows management strategy.

Resources

- Learn how to design your Active Directory by downloading this free chapter from *Windows Server 2003, Best Practices for Enterprise Deployments* at www.reso-net.com/documents/00722343x_ch03.pdf
- Special Operations Software Web site at http://www.Specopssoft.com/
- The Definitive Guide to Vista Migration. by Danielle Ruest and Nelson Ruest
- *Windows Server 2003, Best Practices for Enterprise Deployments*. by Danielle Ruest and Nelson Ruest (Osborne McGraw-Hill, ISBN: 007222343X)
- *Windows Server 2003, Pocket Administrator*. by Danielle Ruest and Nelson Ruest (Osborne McGraw-Hill, ISBN: 0072229772)

About the Authors

Danielle Ruest and Nelson Ruest, MCSE, MCT, Microsoft MVP, are IT professionals specializing in systems administration, migration planning, software management and architecture design. They are authors of multiple books, notably two books published by McGraw-Hill Osborne, “Windows Server 2003: Best Practices for Enterprise Deployments”, ISBN 0-07-222343-X and “Windows Server 2003 Pocket Administrator”, ISBN 0-07-222977-2 as well as “Preparing for .NET Enterprise Technologies”, published by Addison Wesley, ISBN 0-201-73487-7. They are currently working on the “Definitive Guide to Vista Migration” for Realtime Publishers which will be released one chapter per month starting in December 2006.

Les Entreprises
Resolutions Ltd.
Enterprises
www.Reso-Net.com