Realtime publishers

September 2009
Volume 2, Number 9

Windows Administration
in Realtime

Letter from the Editor

What Makes Good IT Content?

by Greg Shields

Above all, Realtime Publishers is a content company. We see our mission as developing the very best content, written by the world's best IT writers. It's content that's on our minds when we wake up in the morning, and it's the last thing we think about as we head towards bed.

Yet content comes in many forms. There's our old friend, the printed word. These days, we've got audio and video mediums with greater fidelity. Podcasts, webcasts, and virtual conferences are all different in the ways that they go about transferring knowledge from one person to another.

Even within a particular content type, there are a lot of ways to *package* that information: Short-form Essentials Series get you the data you need in a few pages, but often without the depth that comes through an eBook like our Shortcut Guides and Definitive Guides. Individual articles in this eJournal are even more concise, often detailing the specific steps that resolve common IT problems.

Many times, it's *finding the right package for that content* that's the hardest part. All of our authors have stories to share. Fitting them into the right package involves a lot more strategy and effort than you'd think.

It is for exactly this reason that our daily posts to the Windows Server Community have come to an end. If you hadn't noticed, on August 11th, it officially sailed into the sunset. That outlet for daily news on the topics, trends, and technology in IT served its purpose for nearly 3 years and 1200 posts. An excellent source for the news of the day, our Windows Server Community quickly became a one-stop shop for all things interesting in IT.

But, as I said before, *we're always thinking about packaging*. You've told us that the information you need is deep. It solves specific problems in IT. It helps you make the right decisions when you're architecting solutions and making purchase decisions. You've told us that you want more than the bite-sized posts that blogs are good for. You need comprehensive IT content, like what you're getting every day on our Nexus site at www.realtime-windowsserver.com.

We've heard your request. It's exactly that kind of content you can expect to begin seeing here at Realtime. Starting this month, you'll start seeing deep discussions on topics like Windows Terminal Services, Group Policy Preferences, and How to Save Money in your Data Center. This solutions-oriented content you'll start seeing on the Nexus site itself, where you need it most.

So, keep an eye on www.realtime-windowsserver.com, because that Web site is about to get a lot more dynamic in the months to come!

Break the Habit

Group Policy

by Don Jones

Most organizations these days rely on Group Policy to some degree, and with good reason: it's an excellent configuration technology; it's convenient, relatively straightforward to use, and each new version of Windows brings better and better support for GPO-based configurations. But Group Policy is also easy to abuse, and doing so can lead to higher administrative overhead, poor performance, and other undesirable conditions:

- Don't leave unused sections in a GPO; instead, disable them. In other words, if a given GPO isn't using, for example, anything in the User Configuration section, then disable that section to speed GPO processing by clients. To do so, find the GPO in the GPMC, click the Details tab for it, and use the drop-down at the bottom of the tab to disable the appropriate portion of the GPO.
- Don't duplicate GPOs if you can avoid doing so. A single GPO can be linked to multiple locations; there's no need to repeat the same configuration settings in a dozen different places. Doing so makes management more difficult when you need to make a change, since you have to change it in multiple locations.
- Minimize GPOs. Every GPO takes time to download, process, and so forth, slowing login and placing a tiny extra burden on domain controllers. Multiple GPOs are fine, but exercise common sense and try to use the minimum number possible. Make it a fight to add a new GPO—don't do it unless you can't argue yourself out of it.

One good reason to have multiple GPOs: When you make frequent changes to settings. Grouping frequently-changed settings into a single GPO will help reduce processing overhead—Windows won't have to re-examine your less-frequently changed settings every time you make a change to your "frequent" GPO.

- Avoid cross-domain GPOs at all costs. Sometimes you might not be able to avoid them, but they do add a lot of overhead to the logon process and place additional workload on domain controllers. It may seem convenient to leave all your GPOs in a single domain and have them apply to many domains, but don't do it. Users and computers should be able to get all their GPOs from whatever domain they authenticate to.
- Measure Group Policy performance. You can do this in Win2008 and Vista by using the new Event Viewer Operational Logs—there's a Group Policy operational log that displays good statistics on how long GPO processing takes. Establish a performance baseline, and re-evaluate it each time you make changes to GPOs to make sure you're not dis-improving performance.

Share your own "worst practices" with Don by asking a question at his Web site, www.ConcentratedTech.com.

Don Jones is a co-founder of Concentrated Technology. Join him and cohort Greg Shields for intense Win2008 and Windows PowerShell training—visit ConcentratedTech.com/class for more details. Ask Don a question by visiting ConcentratedTech.com and using the "Contact" page.

Product Review

PGP Whole Disk Encryption

by Eric Schmidt

As computer hardware improves, laptop and netbook computers have been getting more powerful and less expensive, which has led to sales of portable computers outpacing their desktop counterparts. This increase has resulted in more sensitive personal and company information being stored on devices that are much easier to lose or have stolen. According to one study, 12,000 laptops are stolen from airports every week. One solution to the theft problem is to train users on protecting these devices while at airports or other public locations, but the unfortunate reality is that these thefts will continue to occur. What every company and laptop user needs to focus on is preventing the data from being accessed when these devices are lost or stolen. While a computer is on, data can be protected using access control lists (ACLs); however, when the computer is off, an ACL is relatively ineffective because the hard drive can be removed and mounted on another system that will allow full access to everything. The way to protect data at rest is to encrypt it.

PGP Whole Disk Encryption (WDE) from the PGP Corporation can be used to provide full data protection against unauthorized access to hard drives and other portable storage devices. WDE enables an entire hard drive to be encrypted and requires users to provide a passphrase before the system boots the operating system (OS). This approach provides transparent access to the hard drive for the user while protecting the data if the drive was ever lost or stolen. With WDE, the data is only encrypted at rest; once the passphrase is provided, the data becomes available as it normally would with no additional user action. The

other benefit for end users is that no matter where data is stored on the hard drive, it will be protected when the system is off. For deployment in companies, the application can be centrally configured and managed using the PGP Universal Server product. Data can be recovered by the PGP administrators even if users forget their passphrases.

The WDE process does take a significant amount of time to complete depending on the size of the hard drive, and the process tends to impact performance while running. If it has too much of an impact, the process can easily be paused and resumed at any point so that it can complete at the user's convenience.

Virtual Encrypted Disks are another feature that PGP WDE offers. A virtual encrypted disk is stored as a single encrypted file. When opened, it is mounted like another hard drive so that data can be stored on it. During the creation process, the size of the virtual disk is defined and the size of the file grows dynamically as data is added to it. Although virtual disks can be used to protect data on laptop hard drives and portable devices, it's not as effective as whole disk encryption because data must be stored in the virtual disk in order for it to be protected. The ideal use for virtual disks is for the storage of sensitive data on file servers. Generally speaking, it's not a good idea and may not be practical to whole disk encrypt a file server due to the size of the volumes and the issues that are created when performing backups. Instead of whole disk encrypting a file server, users can create virtual encrypted disks and then store those files on a server. Since the virtual encrypted disk is stored like any other file, it can easily be backed up or copied/moved to another location without any additional effort. The data inside the file remains fully encrypted and protected.

For additional encryption features, PGP also has a suite called PGP Desktop that includes the ability to encrypt email and instant message traffic. PGP WDE and the desktop suite are available for both Windows and Mac platforms. Although the retail cost of $239 for the suite and $149 for WDE may seem prohibitive for companies with a large number of systems, it can be justified by examining the value of the data it protects, making it well worth the expense. All it takes is the theft of a couple systems with proprietary data to demonstrate the value of the product. ◆

Eric Schmidt works as Enterprise Microsoft Security Technologist, with Honors, for Raytheon Company and has worked in Information Technology for 13 years. Eric has a Masters degree in Computer Information Technology and has developed extensive experience in systems administration, engineering, and architecture specializing in Microsoft Active Directory and Systems Management. Eric has been well recognized throughout his career for his contributions to designing and implementing enterprise-wide solutions using Microsoft Windows-based technologies.

Are You Doing Enough to Protect Your Company?

by Lori Cotton

Gaps in security and data leakage due to intentional or unintentional breaches in security can debilitate or paralyze a company. Situations with this severity may result in irreparable loss. Could your company recover?

In an internet-driven business marketplace, risks abound. Businesses both large and small may have the best security solutions implemented and the best policies in place, yet configuration of the solution, enforcement of those policies, and participation by every member of the organization is crucial to the success of your implementation.

Determining Your Level of Risk

Larger companies may choose to use third-party software or to initiate an audit to determine their level of risk. Deciding whether to thoroughly audit using internal resources, third-party software, or to hire a trusted third party to drive the audit is a critical choice that will be made based on finances and/or comfort with allowing outsiders in. Such companies may choose an internal review, consuming valuable resources that could, or should, be dedicated towards other projects. Regardless of the path chosen, it is imperative that the review be thorough and comprehensive to ensure that the solution developed will protect your company.

Critical Factors

The critical factor in a successful security implementation is a solution that ensures that what is developed is enforced. A company may have acquired and implemented the best tools in the business, but if users aren't trained, the result is a useless security posture that leaves your organization vulnerable. Imperatives to success, in sequential order, include:

- Tools
- Configuration
- Policy
- Training
- Adherence

Following an audit, the first three bullets set the stage for success. But without training all members of the organization, and their subsequent adherence to the policy implemented, success is doubtful.

Adherence Is the Key to Successful Implementation

Several aspects of a security implementation depend upon IT and facilities staff and may involve active participation by employees; however, many other aspects of a security implementation depend heavily upon employees and their adherence to policy. To further complicate matters, a combination of physical and electronic risks and solutions to those risks must be addressed.

Web 2.0, for example, introduces many security risks. Social networking sites are often used for marketing purposes or in job searches. In some cases, these sites will be blocked by IT. In other cases, where the sites are used or referenced in marketing activities, various departments will need access to them in order to perform their jobs. The introduction of third-party applications through many of these sites introduces an undercover threat that can expose your company to malicious software.

Several other critical areas to address, concerning both physical and electronic risks, include:

- Avoiding piggy-backing (the technical term for sneaking through a locked or password-protected means of egress behind someone who is authorized to enter)
- Clarifying how to identify, and the proper response to, phishing emails
- Prohibiting, or limiting, the use of personal email from corporate hardware
- Restricting or mitigating the ability to download or install malicious software
- Educating employees about the risks of broad-based Internet use from corporate hardware, and restricting the ability to visit potentially malicious Web sites (to the greatest extent possible)
- Outlining procedures for identifying and sharing protected information with those outside of the company (this could include financial information, customer information, and so on, which may or may not be shared with partners or other organizations for business-suitable purposes)

For companies going about it on their own, the Information Technology Infrastructure Library (ITIL) can provide a reference tool to help an organization conduct analysis and design a comprehensive solution. In other cases, simple Internet searches can enable the development of an audit framework and of course many suggestions for solutions including training. A plethora of vendors, VARs and other service providers are at the ready to provide specific tools and resources at a price, for those who need additional assistance.

The "Human Factor"

As a proof point for the necessity of training as a critical factor in a security implementation, consider the following example: A well-known data encryption company performed a malware test on a large bank not too long ago. Prior to an audit being performed, the company sent an employee to the bank with a handful of thumb drives. The drives were discreetly scattered on the floor of the bank. When the outcome of the test was reviewed, they found that every single drive was picked up by an employee of the bank. Subsequently, each and every drive was plugged into bank computers. Had there been malware on any one of the thumb drives, the result could have been disastrous.

This example illustrates the need for training and adherence as an integral necessity of security best practice to protect against, among other things, social engineering. Social engineering can broadly be defined as a non-technical means of manipulating an unsuspecting individual or individuals into doing something against security policy and procedure (or tricking them into releasing personal or proprietary information). Often, the individuals inflicting such harm will evoke a positive sentiment through either compliment or subtle persuasion, and the recipient is completely unaware of the ulterior motive. Other times, those involved will take advantage of an individual or group's technical or security naiveté in order to circumvent policies and accomplish their goals. Either way, the "human factor" presents a large gap in security policy and procedure that is often very difficult to eradicate. To avoid it means examining the organization with respect to all possible loopholes that could pose a threat to the organization. Areas to evaluate thoroughly include points of egress as well as a complete and consistent communication/response tactic addressing both in-person, electronic, and telephone communication. Addressing these areas equates not only to setting policy and training employees on that policy but actually changing behavior and enforcing the adherence to that new behavior until it becomes second nature. To ensure the behavioral shift, frequent and thorough blind testing is necessary.

Implement, Enforce, Test, Repeat

To bolster the diligence of the implementation, continuous security awareness practices are a must-have. That includes not only frequent testing, communication, and enforcement, but also training and communication for new hires. Often this latter practice is overlooked, creating a potential gap in security procedure between the time that the new hire joins the organization and the time they take their first security-awareness class.

Some argue that any security solution is better than none at all. However, a successful security solution will fully evaluate the level of risk to the organization, considering physical and electronic risks, then incorporate all aspects of security planning and implementation including tools, configuration, policy, training, and adherence. Only then is your company protected. ◆

With nearly 14 years of experience marketing technical products and solutions to both technical and business decision makers, Lori Cotton's strengths lie in the translation of technical features to business benefits and the description and presentation of those benefits to the market. Lori's experience includes the writing of product and solution whitepapers, technical briefs, presentations, articles, and various other marketing collateral covering topics such as networking, security, and services. Companies for which Lori has written include Fortune 100 and 500 companies such as Intel, BATM, and CA as well as smaller companies such as Shiva and OpenReach. Lori's expertise stems from a background in product marketing and product management.

The Deep Dive

Three More Popular Posts from the Realtime Windows Server Community

by Greg Shields

With the conclusion of daily posts to the Realtime Windows Server community (www.realtime-windowsserver.com), I'm dedicating this month's Deep Dive column to extending its memory just a bit more. This month, I present you with three more posts that you have recognized as critically important above all others.

Back in the August issue, I presented you with our most-popular post based on your inbound page count. That tip provided you with the Officially Correct Process to Use ESEUTIL & ISINTEG Against a Busted Exchange Database. Yet that post was only one of nearly 1200 penned in the last two-and-a-half years. Of those innumerable posts, three more stand out as most-useful tips and tricks for making your IT job just a bit easier.

Migrating Outlook Autocomplete Data (NK2 File Data) to a New Vista/Office 2007 Computer

I'm in the process now of moving all my data over from my old computer to my new computer and remembered that autocomplete information is not stored in the Outlook profile. Autocomplete is the drop-down suggestion window that appears when you start entering in an address in the To, CC:, or BCC: bar. Like you, this data is something I can't live without.

That data is stored in an NK2 file that for previous (non-Vista) OSs used to be stored in C:\Documents and Settings\{username}\Application Data\Microsoft\Outlook. Note that this location is not where your Outlook profile

is by default stored. That location on non-Vista OSs is C:\Documents and Settings\{username}\Local Settings\Application Data\Microsoft\Outlook. Notice the difference in the two paths: the second includes traversal through the "Local Settings" folder.

Now, in Windows Vista, that folder doesn't exist. So, I had problems finding it.

Turns out that the new location in Vista where your NK2 file is located has moved to fit it into the new structure. That new location where you need to copy the NK2 file is C:\Users\{username}\AppData\Roaming\Microsoft\Outlook.

Outlook 2007 RSS Feeds Not Updating: A Solution

Over the past couple of weeks, I've been struggling with Outlook 2007 and its RSS feeds. I first maxed out the limit of my PST file and learned that I needed to do a manual export and import into an Outlook 2007-style PST file that can handle more than 2G of data.

That was the first problem.

Once I completed that lengthy process, the next thing I found was that my RSS feeds within Outlook no longer updated properly. Making the problem even worse, I found that Outlook no longer even recognized most all of them when attempting to reset Send/Receive settings. So, I promptly ignored the problem for a couple of weeks, knowing I didn't have the time (or didn't want to make the time) to seek out a fix.

This morning I finally hit the wall and started looking for a resolution, which I found.

Like a lot of people, I use Internet Explorer (IE) to connect to new feeds and expect Outlook to pick up any new ones automatically.

Turns out that there are two or three files in your Windows profile that directly relate to Outlook's RSS feed synch inbound from IE. On a Vista machine, look in the folder C:\Users\{username}\AppData\Local\Microsoft\Outlook. There, you'll find two or three files named: outlook.sharing.xml.obi, ~last~.sharing.xml.obi, and outlook.xml.kfl.

Completely guessing here, but outlook.sharing.xml.obi is the file that determines the feed structures Outlook shares with IE. The file with the ~last~ name I assume is some sort of locking file while Outlook is running. Finally, the outlook.xml.kfl file includes (according to the file) "known CFL feeds to Outlook."

What happened, it appears, is that when I completed the export and subsequent import, that process caused Outlook to lose its brains as to the connection with IE's feeds. These files drive that connection, and are re-created if not present every time Outlook starts.

So, the process to fix the problem was to shut down Outlook, remove these three files, and restart Outlook. Immediately, Outlook synched with IE, brought down the RSS parameters, and began updating again. If I read these two files, I now see that instead of being relatively empty, they now include feed characteristics for all my feeds.

The only bad part about this process is that data from my previous feeds was already in my PST. So, Outlook created all new folders with a trailing (1) in the title. I had to delete all the old data and rename the folders again, but with only about 50 feeds, this didn't take too long.

Has this worked for you? Have you seen this problem? I had a heckuva' hard time finding this solution, so I wanted to share.

Location of WSUS Log Files

If you've been having trouble locating the root cause of problems with your WSUS infrastructure, be aware that a number of log files are available at both the client and server:

- The Windows Update Agent has a log file "%windir%\WindowsUpdate.log" with verbose logging on updates that have been installed.
- WSUS 3.0 has a log file "%Program Files%\Update Services\LogFiles\changes.log" that contains a record of all recent approvals and who made them. If the approval was created automatically (e.g., auto-reapprove revision, auto-approval rule, or auto-approve WSUS updates), the user in the log will be "WSUS Service."
- A third log file on the WSUS server itself is "%Program Files%\Update Services\LogFiles\SoftwareDistribution.log." This log provides information about the software updates that are synchronized from the configured update source to the WSUS server database.

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.

Exclusively Exchange

On-Premise vs. Hosted Email Security

by J. Peter Bruzzese

The evolution in software delivery models offers us new options, as well as challenges, in terms of selecting the most appropriate, functional, and user-friendly applications for business environments. In the area of security, messaging is arguably the most sensitive information service in a company's software suite. With messaging downtime, corporate data loss, and financial threats being major concerns for any business, a messaging security solution that is truly secure, easy-to-use, and non-disruptive is a must.

If a company becomes affected by an email borne threat, creating a situation where employees cannot send communications through email, what is the end result? When business, marketing, sales, customer support, and operations come to a screeching halt, imagine the damage. The result is a loss of revenue and possibly harm to the brand.

To protect against threats that originate from email, the Exchange or IT administrator can approach security in one of two ways: 1) by deploying an on-premise solution, whether it be an appliance or software, or 2) by contracting with a hosted provider that will filter and secure your email. The method you select really depends on a variety of external forces at times. It may depend upon company culture, markets, operations, and business models, as all companies have disparate IT requirements. Therein lies the challenge between selecting an on-premise versus a hosted email security solution. Each approach has pros and cons to be considered. In determining which approach best fits your business, consider the following dozen guidelines you can use as part of your selection process:

- Everyone is looking for a solution that offers a lower total cost of ownership (a solution that doesn't require upfront capital investment, ongoing administration, and/or user training)
- Another plus is a solution that doesn't consume large amounts of IT or administrative resources to maintain effective performance
- Some solutions provide rapid detection and response to new virus and spam outbreaks (perhaps as a result of community learning)
- Determine whether you require complete control or can hand off some (not all) of the control to a hosted solution
- Figure out whether your proposed solution preserves network and server bandwidth as well as storage space
- Your preference in how security threats are processed—inside or outside the corporate perimeter
- Fastest time to value delivery—can the solution be deployed and working quickly?
- Determine whether your proposed solution will introduce a new single point of failure within your email infrastructure
- Interoperability with existing network systems and software
- Multiple layers of protection against spam, malware, phishing, viruses, vulnerabilities, and other attacks
- Simple operation and management to reduce IT burden and allow focus on more strategic IT initiatives
- Very little or no user training requirements

Of the two approaches to address email security, on-premise solutions are arguably the most popular. Why is that?

On-Premise Email Security

Although on-premise email security has historically consisted of software installed on a server inside the corporate network with the processing of email threats occurring within the walls of the organization, hardware-based email security appliances are available and utilized in many organizations as well. Let's consider the pros and cons of these solutions.

Pros

On-premise email security (hardware- or software-based) can effectively protect against spam, viruses, and other email threats. On-premise does provide a perceived sense of control because email data stays within the business' walls and you can manage these systems onsite. You can mitigate some of the risk by putting your filtering solution (for example, your Edge Transport server role in Exchange 2007) in the DMZ; that is, your perimeter with a firewall in-between the solution and the functioning network.

Cons

Because both hardware and software deployments allow email-based threats to enter the walls of the business before being stopped, the business is at risk from attacks by malware and viruses. Also, there are bandwidth costs to hosting email security software on-premises, plus the upfront costs of the software licenses and dedicated spam-processing servers. In addition, cost is a factor with an on-site solution. It requires considerable upfront capital, ongoing maintenance fees, and daily IT administration (monitoring and so forth). Furthermore, these security solutions (appliances or filtering servers) must be integrated into the overall network for interoperability, which provides for a new point of failure.

Hosted Email Security

As a counter to on-premise solutions, hosted email security processes email threats outside the corporate perimeter, so malware, botnets, and phishing threats can be sorted out before delivering email to the internal Exchange or other email server. In explaining their approach to cloud-based email security, David Setzer, CEO of Mailprotector (http://www.mailprotector.net/), an email and Web security company in Greer, SC said "Keeping threats off the corporate network should be viewed as a best practice that will not only protect email availability, but support business continuance. On-demand email security services, like that offered by Mailprotector, keeps threats originating from the Internet offsite while reducing the IT management burden." Let's look at some pros and cons.

Pros

Hosted security services require no capital expense or ongoing maintenance costs for hardware and software, although of course you pay for the service through an ongoing subscription charge. There is also less of a need for IT training because companies that offer hosted email security are staffed by full-time security professionals who do the work that internal IT staff normally would.

Cons

The perceived loss of control because email is processed externally by someone else. In fact, for some organizations, this may be a deal breaker in that your company policy may have a big x across this kind of option depending on the type of business.

Hosted Solutions: Where Do I Stand?

It's obvious I have a leaning here toward the hosted solution. As an Exchange guy, I'm typically anti-hosted solutions because I like having the servers under my own thumbs so to speak. But as time progresses and hosted providers become more and more trustworthy, I'm beginning to let go of some of my control issues. I was surprised in a recent Techmentor Conference when I asked the audience what they used, several said they kept Exchange in-house but used a hosted security provider, keeping all the spam and such out of their business network, handled in the cloud. It made sense. Now there were some in the audience who preferred to keep it all under their realm of responsibility. But I could tell that there were others in the audience who felt the burden lifted of caring for an Edge Transport server. They just needed to know it was "OK." They weren't any less of an Exchange admin by outsourcing their security to a hosted provider. For some of us, it is time to let go… just a little… if it is a good fit for your company. Less time worrying about spam filtering may give us more time for 18 holes of golf.

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. In harmony with the joy of writing Exclusively Exchange for Realtime Publishers, he has created a free Exchange training site at www.exclusivelyexchange.com. His most recent book "Exchange 2007 How-To" was published by Sams in January 2009. He is co-founder of ClipTraining.com, a provider of short, educational screencasts on Exchange, Windows Server, Vista, Office 2007 and more. You can reach Peter at jpb@cliptraining.com.

Copyright Statement