Realtime
publishers

October 2009
Volume 2, Number 10

Windows Administration

in Realtime

Letter from the Editor

Get Off the Freaking Console!

by Greg Shields

Again and again I find myself repeating that statement when I'm out presenting at conferences or consulting for businesses. Fellow admins, it's nearly 2010, and its time to starting thinking client/server when we administer our servers from our clients.

What am I talking about? I'm talking about the process of performing systems administration from the console of our servers. Whether we walk over to the data center or we remote in via Terminal Services or another utility, doing systems administration directly on our servers' consoles is the IT equivalent of hooking up a team of horses to get your Ferrari around town. It's archaic, it's wasteful, and it's terribly hard on the horses.

Console-based administration has a long history in IT, dating back to the first Windows operating systems (OSs). Unlike telnet with their UNIX brethren, our Windows servers didn't always have remote console capability. Working with those servers usually meant donning our coats and spending time in a cold and lonely data center.

Yet today's Administrative Tools for Windows XP and Remote Systems Administration Tools for Windows Vista and 7 are very complete in the offerings they provide at your desktop. Completing the suite are scripting languages such as VBScript and PowerShell. There are precious little management tasks you can't accomplish today using some combination of lightweight tools and scripting right at your desktop's fingertips.

Why stand on my soapbox today on this particular topic? Why is console-based management, the de facto standard for so many years, now taboo? One word: Virtualization. Today's virtual environments spend cash and effort into getting as many virtual machines to successfully run atop a single physical host. We nip, and tuck, and optimize in whatever way we can to eek out as much performance as possible for those virtual machines.

Then, we log into that computer to administer it and screw the whole thing up.

The result of a login is dramatic to the virtual environment. You can argue that the simple process of logging into a server consumes more resources than any other action accomplished on that server. All those resources—disk, memory, processors—are needed during a very short time to process the login, create the explorer shell, and create an operating environment for you, the admin. All completely copacetic when servers run at 5% utilization, and all fully wasteful when resources are precious.

I'm a mountain biker, and have been for nearly 15 years. This story reminds me of a similar situation I find all the time on the trails here in the mountain west. You find fellow trail riders with the highest dollar bikes money can buy, the lightest component set, and tires with ten ridiculously-expensive military-grade spokes instead of the usual 36. And after you appreciate the fine machine they've spent a mortgage payment (or two) making theirs, you look at the rider and think, "All that money spent, and you'd save more weight by simply not eating that cheeseburger for lunch."

My friends, our lives as IT professionals are difficult enough. Make your job just that much easier and learn to do it truly remotely. I promise you'll appreciate the result. ◆

Break the Habit

Buying the Hype

by Don Jones

Buying the Hype

Whenever Microsoft releases a new operating system (OS)—or even a service pack with a major new feature—you've got to be a bit careful. Especially when the feature is disabled by default, you really need to ask yourself why that is and whether you should be enabling it. I, unfortunately, see too many administrators make decisions—that are often irreversible—simply because they're excited about a new feature they've heard about but that they haven't had time to really research.

An excellent example of this is the new Active Directory (AD) "Recycle Bin" in Windows Server 2008 R2. I'm not here to tell you it's a bad feature; I am here, though, to tell you that it may have been a little over-sold and that it's absolutely not appropriate for every environment in the world. It is disabled by default, which should give you some pause, and enabling it is a one-way decision—so you'd better be sure it's right for you.

When Is a Recycle Bin Not a Recycle Bin?

When you say “Recycle Bin,” I immediately think of Windows Explorer: An automatic feature that lets me retrieve deleted files using a simple graphical user interface (GUI). Outlook has a similar Recycle Bin, and in fact, you get a similar experience everywhere Microsoft uses the Recycle Bin metaphor. But that’s not quite the case with AD.

First, the requirements: The Recycle Bin can only be enabled in domains that are operating at the 2008R2 functional level, meaning all your domain controllers need to be upgraded. R2 is only available in 64-bit, meaning it can’t be used to upgrade any 32-bit installations and it can’t be used at all on any older 32-bit hardware—which may include 32-bit virtual machines. So, for most organizations, it’ll be quite some time before the new “Recycle Bin” is even an option. You may well have to reinstall domain controllers from scratch or deploy new ones and decommission old ones before you can even make the decision! If you do make the decision to enable the Recycle Bin, beware: You cannot turn it off again. This is a one-way decision.

So how does it work? Normally, when you delete an object in AD, it’s marked with a “tombstone,” which effectively hides the object and renders it useless. That tombstoned object remains in the directory for quite some time, ensuring that every domain controller—even ones that may have been briefly offline—receive the replication activity that deleted the object. It’s possible to remove the tombstone and “reanimate” the object (I love the graveyard jargon) but most of its attributes will be gone because AD doesn’t retain the attributes of tombstoned objects. So reanimating may be accompanied by a lot of manual work to re-populate attributes.

The new Recycle Bin, once enabled, creates a new, normally-hidden container. Now, when objects are deleted, they are copied into this “Recycled” container with their attributes intact. Retrieving the objects still requires special tools (like the LDP tool), because there isn’t actually a graphical “Recycle Bin” in any of the AD tools. However, if you do retrieve an object, its attributes will be intact.

This can actually present a problem for some organizations because AD attributes—especially for users—may well contain personally-identifiable information (PII), and some organizations *aren’t permitted* to retain that information past the time of an object’s deletion. For those organizations, it’s critical that the Recycle Bin not be enabled. You may prefer to obtain “recycling” capabilities from third-party tools that can properly secure deleted objects and manage PII retention in accordance with your company’s particular needs.

The lack of a graphical “Recycle Bin” in the AD tools is, frankly, astonishing. I’ve always felt that the native AD tools were the bare minimum Microsoft thought they could get away with, and this doesn’t change my opinion. I’m not sure what reasoning would be behind offering a “Recycle Bin” feature without exposing a Recycle Bin icon somewhere in the tools. Third-party solutions that provide single-object recovery nearly always provide a standalone or integrated interface, and it just seems weird that Microsoft wouldn’t do so as well. To be fair, Microsoft *primarily* bills this new feature as “Deleted Object Recovery,” but it’s been colloquially referred to as “Recycle Bin” in enough articles and TechEd presentations from AD team members that the world in general now has an expectation for the feature that doesn’t quite map to reality.

Such caveats are common accompaniments to new Windows features, though, and it’s why you should always investigate thoroughly before jumping in with both feet.

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 - Part I

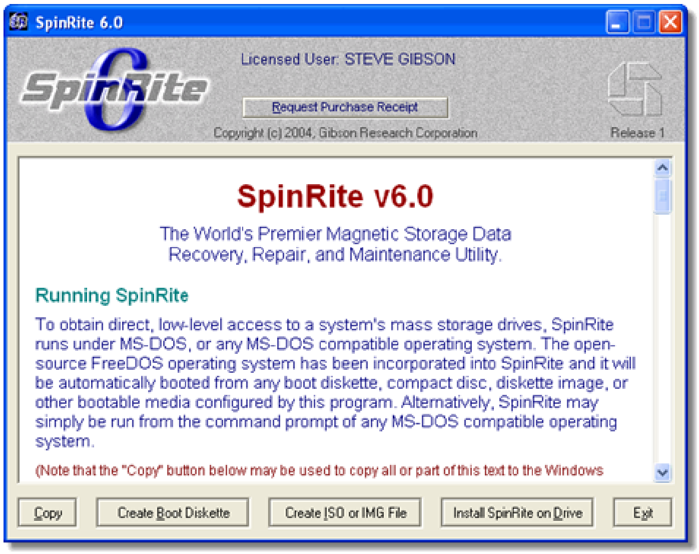
SpinRite

by Eric Schmidt

Hard drives have continued to grow in capacity to incredible sizes that were unimaginable a decade ago. With capacities so great, a substantial file server could be created by throwing a couple inexpensive 1.5 terabyte hard drives in a workstation. The fact that drives have gotten so large for desktops and laptops means that users are not presented with the storage limitations that would force them to use a company file server a decade ago—which is a VERY bad idea. Without proper education as to the importance of saving files on a fully redundant server with daily backups, users are likely to store important data locally. Laptops present a similar but greater problem because those devices are not always connected to the company network, so users often choose to store data locally so that they can access it from anywhere. Laptop hard drives are also more susceptible to errors and failures because they are portable and can easily be dropped or mishandled.

At this point, one might think that this product review would be focused on a backup or encryption product; however, there is another data loss risk that is of equal importance if users store significant amounts of data locally: hard drive failure. Concurrent with the exponential increases in capacity, there have been many advancements that make hard drives more reliable than ever before—but they are still mechanical devices that can and do fail. When they fail, it may be essential to recover as much data as possible. The traditional way to accomplish this task is to send the drive to a company that specializes in data recovery where the drive is opened in a clean room and the data is directly recovered from the platters. This option is very expensive and in many cases is not necessary because hard drives generally don't completely fail to the point where they are totally inoperable. This is where an application called SpinRite by Gibson Research Corporation can be leveraged to recover data on a failed drive at a fraction of the price of the traditional "clean room" data recovery services.

The first feature of SpinRite is that it's a very small self-contained executable that requires no installation. Running the executable opens a simple interface that is used to create bootable media (CD or USB drive). The computer with the failed or questionable hard drive is then booted to that media so that the scan and recovery can be performed. After booting to the removable media, the application presents a very simple interface that allows the user to perform a scan. While the scan is being performed, the application displays an almost-overwhelming amount of information about the drive, including the number of bad sectors. When bad sectors are found, SpinRite attempts to recover the data by moving it to good locations on the drive.



SpinRite v6.0

The World's Premier Magnetic Storage Data Recovery, Repair, and Maintenance Utility.

Running SpinRite

To obtain direct, low-level access to a system's mass storage drives, SpinRite runs under MS-DOS, or any MS-DOS compatible operating system. The open-source FreeDOS operating system has been incorporated into SpinRite and it will be automatically booted from any boot diskette, compact disc, diskette image, or other bootable media configured by this program. Alternatively, SpinRite may simply be run from the command prompt of any MS-DOS compatible operating system.

(Note that the "Copy" button below may be used to copy all or part of this text to the Windows

Figure 1: SpinRite Media Creation Interface.

SpinRite is not only a data recovery utility but also a maintenance and diagnostic utility. In a video on the Web site, Steve Gibson and Leo Laporte discuss and recommend running SpinRite on a monthly basis. The benefit of running it proactively is that it can be used to detect and correct potential issues that have yet to surface during normal computer use. By using it in a proactive mode, data can be moved before a failure occurs.

The product uses the FreeDOS operating system (OS) to boot the system and run the application. SpinRite was written in such a way that it works at the physical media level to read the drive, so it is capable of recovering data regardless of the OS or file system that the drive was formatted with. If the hard drive still spins, it's very likely that SpinRite can recover the data on it. This is due in part to a statistical technique that the documentation discusses, which enables the application to figure out what should have been on a sector that has gone bad or is difficult to read. Once it figures out what should have been there, it moves the data to a good sector on the drive. As with any low-level activity, the SpinRite application can take a significant amount of time to complete, but it is well worth the wait. According to a video demonstration on the Web site, a 100GB hard drive will take about 6 hours to complete.

SpinRite is an outstanding product for performing data recovery and proactive maintenance on hard drives and is a valuable addition to any troubleshooting toolkit for enterprise support staff and consultants alike. ◆

Product Review - Part 2

TrueCrypt

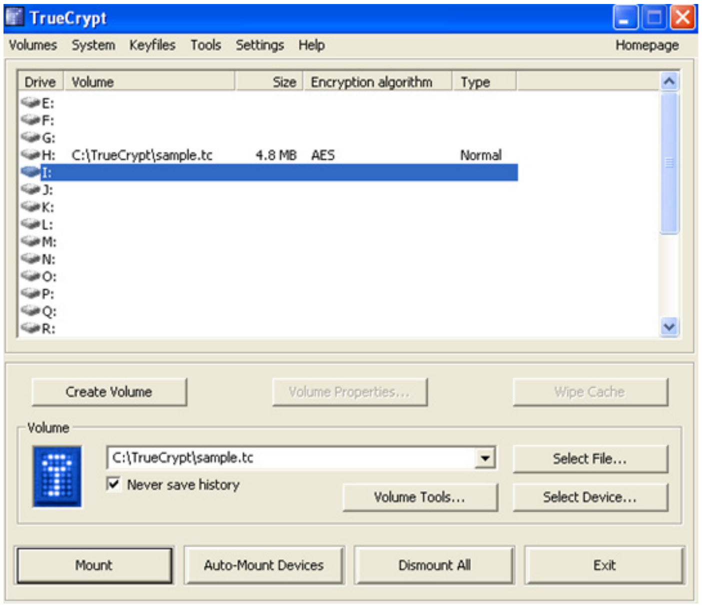
by Eric Schmidt

Portable computers have increased in popularity and with the arrival of the netbook form factor, they have also become very affordable. This shift has resulted in more people using these types of computers as their primary workstations; as such, they are storing more sensitive data on them. Enterprises are also taking advantage of the lower cost and mobility that they offer, which has resulted in more company data being stored on them. This of course has created a potential gold mine for identity thieves and individuals that want to steal company-sensitive information. When mobile computers first emerged, they were stolen for the hardware because they were so expensive. Now that they've become relatively inexpensive, thieves are more interested in the data that they contain. Data theft isn't limited to mobile computers. Portable storage devices have also increased in capacity and decreased in physical size and cost, which makes them very easy to lose. These portable storage devices often accompany mobile computers as a means to back up critical data when on the road.

There are a number of pay products available that provide data protection using encryption. Although they have robust features, their license costs can be prohibitive. A viable alternative to these pay products is a free, open source application called TrueCrypt. TrueCrypt offers a number of ways to encrypt data depending on the need. The first method is to create a virtual encrypted disk. This type creates a single file that, when mounted, appears like a hard drive. This is very convenient for making encrypted data portable because the file itself can be moved around and then anyone with TrueCrypt and the password can open it. This is particularly beneficial for storing encrypted data on file servers because it eliminates the need to encrypt the native file server volume. Virtual encrypted disks are also very simple to back up because the virtual encrypted disk is just like any other file.

TrueCrypt also offers the ability to encrypt entire volumes (hard drives or USB drives). This method is ideal for USB drives, which can easily be lost. However, there is an issue with encrypting the entire drive. According to the TrueCrypt Web site, the best way to encrypt USB devices is to use the virtual encrypted disk and store the file on the USB drive. This method allows TrueCrypt itself to be stored on the drive, which can then be launched on any system without having to install the application. If the whole drive is encrypted, the application must be installed on the system in order to access the data. Entire-volume encryption can also be leveraged for the internal laptop drive and using pre-boot authentication, a password will be required to boot the system.

TrueCrypt offers another feature that will completely hide the encrypted volumes or operating system (OS). This is referred to as plausible deniability. With this feature, the TrueCrypt volumes will appear as random data and cannot be identified as an encrypted file or volume because there is no signature. OS volumes can be hidden with this method as well, which makes its existence completely unknown to everyone except the user who created it.



Drive	Volume	Size	Encryption algorithm	Type
E:				
F:				
G:				
H:	C:\TrueCrypt\sample.tc	4.8 MB	AES	Normal
I:				
J:				
K:				
L:				
M:				
N:				
O:				
P:				
Q:				
R:				

Volume: C:\TrueCrypt\sample.tc

☑ Never save history

Figure 1: TrueCrypt user interface with a sample virtual drive mounted.

TrueCrypt is available for Windows, Mac, and Linux with a simple installation and user interface. The installation also assists users that aren't familiar with the product with a prompt to open a tutorial. TrueCrypt has an outstanding support Web site with a detailed FAQ that provides answers to a wide range of questions about the product's features. For individuals and companies looking for an inexpensive but effective way to provide data protection for mobile computers and storage devices, TrueCrypt is an excellent alternative to expensive commercial products. ◆

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.

The Deep Dive

Service-Centric Monitoring and All the Butterflies in Peking

by Greg Shields

Not too many years ago, I used to work as a Senior Systems Engineer for a major defense contractor. As part of that job, I was responsible for building the email system for the United States' next-generation weather prediction satellite constellation. Although the email server was a relatively unexciting implementation, hob-nobbing with the top rocket scientists in the country absolutely was.

While there, I once asked the Chief Engineer for the program about weather prediction, and the old saying I heard back in grade school, "You can never predict the weather. There are just too many variables at play. The butterfly beats its wings in Peking, and that causes tornadoes in Kansas." Remembering that saying one day, I asked this person, "So, how are we going to predict the weather better than the satellites that're already in orbit?"

His response, which I will always remember, was, "Well, Greg, just imagine if we could watch every butterfly's wings…"

That story got me thinking a lot about an eBook I wrote for Realtime Publishers not too long ago. The Shortcut Guide to Virtualization and Service Automation attempted to explain how an effective service-centric monitoring platform could alert on and maybe even predict failures as or before they happen. Connecting such a system to your data center would net you terrific gains in visibility across your entire environment. (You can download a copy of the eBook from this URL: http://nexus.realtimepublishers.com/sgvsa.php.)

There are a few sections in that eBook that I want to share with you here because they remind me of the whole idea of measuring enough butterfly wings. Essentially, if you have enough monitoring integrations in place, you can do the same with your data center. The resulting service-centric monitoring can be dramatic to your overall ability to proactively manage your environment. Think about this as you read through this extended quote from Chapter 4 of that eBook.

A service-centric management platform's level of monitoring integration into each element—and its visualizations of the result—is much more defined than simply answering the question, "Is 'The Storage' up right now?" In the service-centric approach, the goal of any particular integration is to collect large amounts of data about the IT component as well as an understanding of its underlying health. That understanding can come through the analysis of one of many factors, including availability information, event log data, and performance measurements. For any of these, when conditions occur that are known to effect server and service quality, service-centric management tools will notify personnel in the way described earlier. The end result is a much quicker call to action when problems occur, and in many cases, a pre-failure notice that a problem may soon occur.

In the service-centric approach's bottom-up view, these three elements work together to identify a component's statement of health. Based on rules that are input into the monitoring platform, the movement of any or all of these components away from nominal behaviors will result in a change in health status. Figure 4.4 shows an exploded view of how this might work within our example. In this case, the cause of the example's problem expands a bit to recognize that "The Storage" itself is not necessarily down. By digging deeper, the performance counter for Disk Read Rate is exposed to be above the desired level. Such can be the case when too many virtual machines share disk spindles and are trying to read too much data all at once. In this case, the service's health indicator changes to red to notify administrators of the problem.

With this change, the service-centric management platform will next notify users and may suggest resolutions for the problem. One solution for this problem is to migrate the offending virtual machine's disk files to an alternative disk location where the files do not cause spindle contention with other virtual machines. In the case of highly evolved service-centric management platforms, this solution may be automatically invoked by the system to auto-resolve the problem with no or minimal administrator involvement.

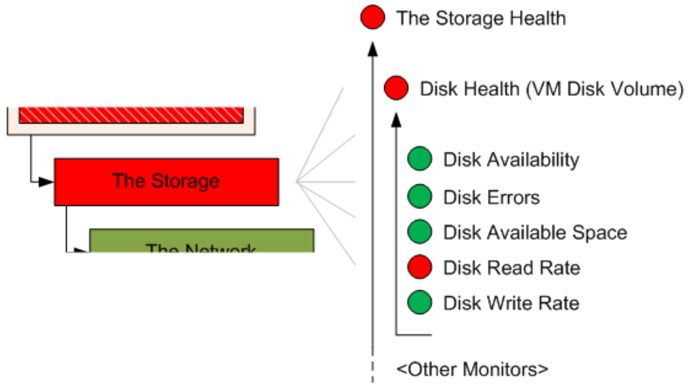


Figure 4.4: This exploded view of the previous figure shows how an identified health failure can be drilled down even further to find its root cause.

With all its capabilities, bottom-up monitoring provides but one perspective of your virtual and physical environment. It enables the easy creation of rollup reports that quickly point troubleshooting teams to problems. Yet with all its power in digging through volumes of data to find the exact source of a problem, it does not provide a good sense of how that service is working from the perspective of the user.

Consider the failure situation Figure 4.5 shows in which users employ a virtualized Web server to accomplish their daily business. That Web-based service relies on two other virtual servers for its processing. All data that the Web server renders to a user starts in a separate database, but must first process through a third application server. In this case, the Web server is dependent on the application server, while the application server is dependent on the database. All servers are dependent on the network for their intercommunication, and all servers are part of the same virtual platform infrastructure. In this fairly common situation, an outage of any of these three servers will immediately result in an outage to the service.

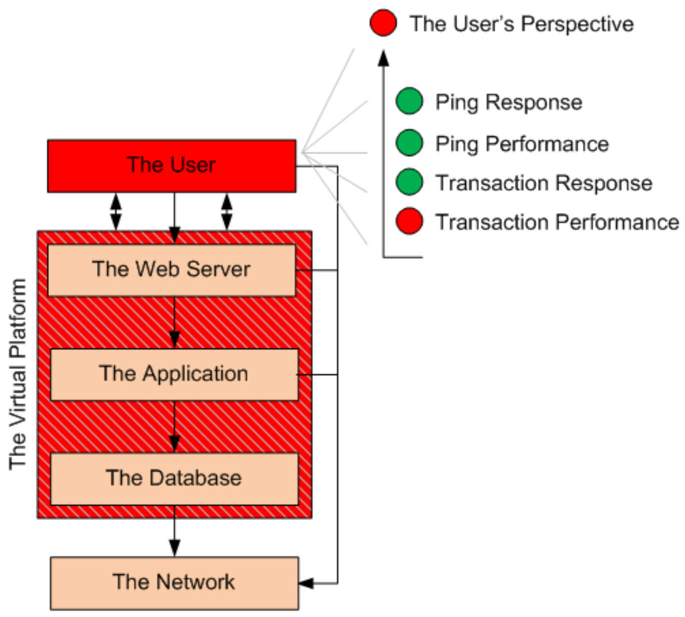


Figure 4.5: The top-down perspective of the service-centric approach looks at the user's experience with applications. In this case, the service's health is poor because of measured client-based transaction performance.

I find myself turning back to these words a lot lately because they remind me how much power we can have at our fingertips. But that power only happens when you can properly monitor your environment. A service-centric monitoring solution's bottom-up approach rolls up low-level behaviors, letting you know before they become big problems. Its top-down approach gives you detailed information about your users and the experiences they're having with your systems—a perspective that is often lost in siloed solutions.

In short, with the right tools in place, it seems you can watch every butterfly's wings. Maybe that Chief Engineer was onto something so many years ago…

Greg Shields is an independent author, instructor, and IT consultant based in Denver, Colorado, and a co-founder of Concentrated Technology. With nearly 15 years of experience in information technology, Greg has developed extensive experience in systems administration, engineering, and architecture specializing in Microsoft systems management, remote application, and virtualization technologies. Greg is a Contributing Editor and Columnist for TechNet Magazine and the author of five books. Greg is also a highly sought-after instructor and speaker, speaking regularly at conferences like TechMentor Events, and producing computer-based training curriculum for CBT Nuggets. Greg is a recipient of Microsoft "Most Valuable Professional" award with a specialization in Windows Terminal Services.

Exchange Server Remote Connectivity Analyzer

by Ron Barrett

So you installed Exchange Server 2007, added all the necessary roles, and configured your Client Access Server (CAS) for external email communications. You checked the log files, services, and everything else you could think of and it is all working great, except it isn't. Somewhere out there on the Internet is a user from your organization trying to get access to their email remotely but they cannot connect to Exchange…now what?

As good as the tools for Exchange Server 2007, there are some areas where the tools within your organization will fail to provide accurate information. One of the areas where this holds true for the Exchange administrator is remote connectivity. The biggest problem is that many times this issue is not immediately apparent when you are running checks within your environment. After deploying the CAS role in Exchange 2007, you would generally test to make sure that all is going well. But remote connectivity is not affected by only the Exchange Server and specifically the CAS server alone: Several factors can cause an issue with remote connectivity, and you might never know without having a screaming user on the other end of the phone.

Thankfully, there is a tool for the Exchange administrator that can help solve this problem and ensure that all is working as it should. The tool is called the Exchange Server Remote Connectivity Analyzer (ExRCA). So what is this tool and exactly how can it assist the Exchange administrator? Let's begin by looking at where things can go wrong; we can then consider how we can use ExRCA to resolve the issues.

Everything Looks Fine, So Why Can't I Connect?

What are issues that can prevent a user form connecting through to the CAS and retrieving email? Five areas that you should consider for testing include:

- Client
- Firewall
- DNS Server
- Certificates
- Reverse Proxy Server

The issues that come up in relation to these areas are changes in the ports on a firewall. Perhaps a port that should be open is not, or if CAS was previously working, the port may have been accidentally removed or disabled in your firewall.

External DNS issues are a big problem for remote connectivity. This is especially true when you need to have your ISP set up your MX records. If there is a mistake in the hostname or IP address, that mistake can create issues. This is a prevalent issue for those who change ISPs and therefore need to change the MX record for their organization.

Invalid certificates are another big issue. Perhaps the wrong type of certificate was requested or the common name does not match. Again, as this is an external issue, all would look well inside the organization.

Another issue arises if you use a reverse proxy within your organization. A wrongly configured reverse proxy would block access for remote users.

Many times, especially in enterprise environments where IT job duties are segmented, it could be quite a task to trouble shoot this matter. If you are only the Exchange administrator, you would need to contact someone from the WAN team to test out the DNS issue. Another call would be needed to the security team to check the firewall port settings. If you use reverse proxies, this task could be handled by another administrator. Certificates could be yet another department, or you may need to contact your Certificate Authority (CA). Finally, the Help desk team would need to deal with the possible end user issues.

How ExRCA Helps

ExRCA is a tool that performs tests against all these possible failure points from outside your network infrastructure. This allows you to get true results and identify where the failure point is so that you can take the necessary steps to correct the issue. This tool allows you to test issues without needing to get every department involved. You can run the tests, find the issue, and work directly with the correct department to resolve the issue quickly. ExRCA currently tests the following remote connectivity options:

- Microsoft Exchange ActiveSync Connectivity Tests—In the Exchange ActiveSync with AutoDiscover (Windows Mobile 6.1) test, the tool will try to synchronize a mailbox via ActiveSync after obtaining the settings from the Autodiscover Service. In the Exchange ActiveSync (Windows Mobile 5.1 and third-party devices) test, the tool will run through steps necessary to connect to your Exchange Server using Exchange ActiveSync.
- Microsoft Exchange Web Services Connectivity Tests—The ActiveSync Provider AutoDiscover test will go through the steps needed for an ActiveSync device to obtain its settings from the AutoDiscover service. The Outlook Provider AutoDiscover test will go through the steps needed for Outlook 2007 to obtain its settings from the AutoDiscover service.
- Microsoft Office Outlook Connectivity Tests—The Outlook Anywhere with AutoDiscover test will try to obtain its settings from the Autodiscover Service and then logon via Outlook. The Outlook 2003 RPC/HTTP test will try to connect an Outlook 2003 client via RPC/HTTP.
- Internet Email Tests—The Inbound SMTP Email test walks through the steps an Internet email server would use to send inbound SMTP email to your Exchange Server.

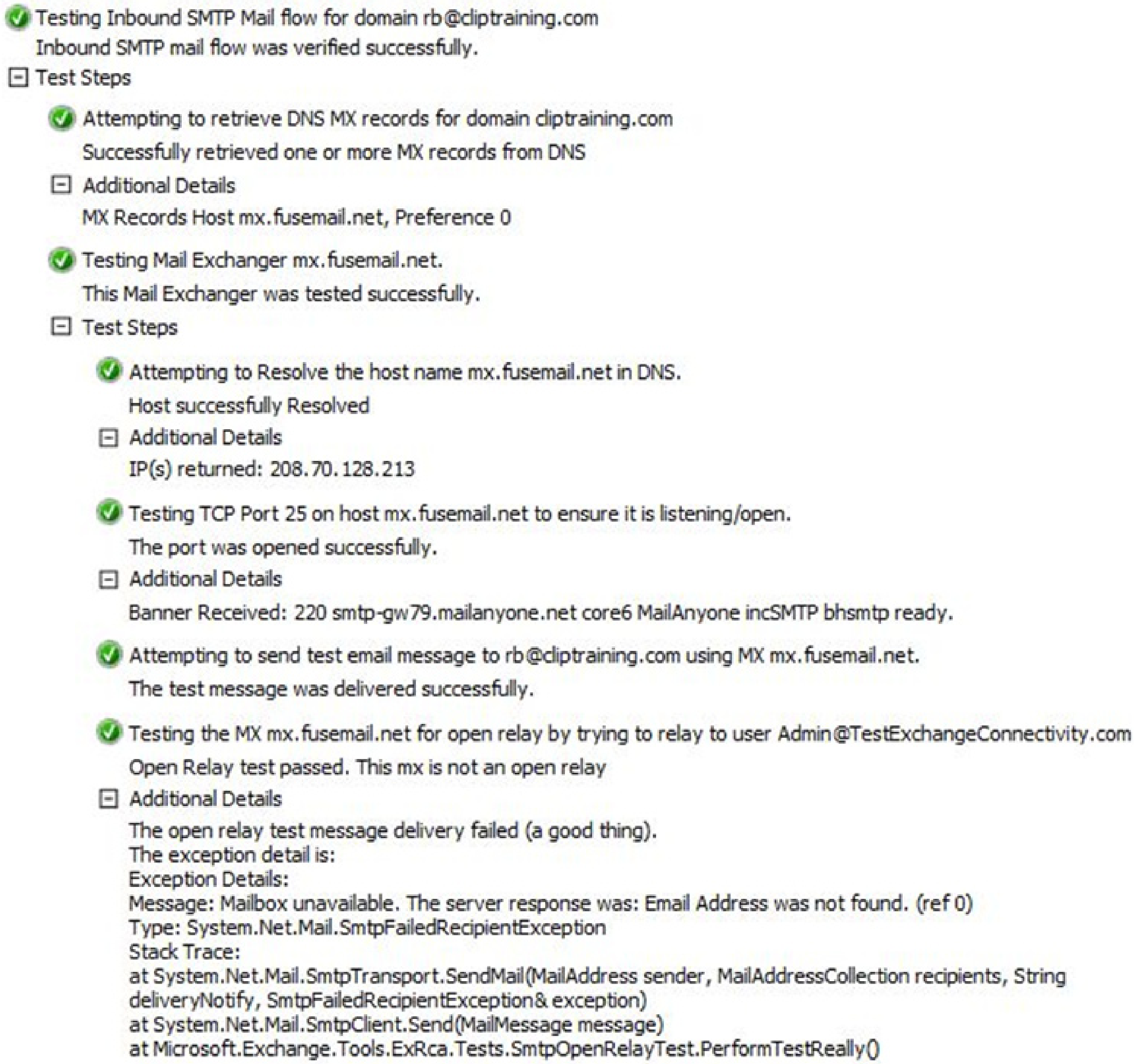
Using ExRCA

To use ExRCA, simply point your Web browser to https://www.testexchangeconnectivity.com/, then choose the test you want to perform, and click Next. Based upon the test you chose, you need to provide the following information:

- Email Address
- Domain /Username or UPN
- Password

Depending upon which test you choose, you will also need to provide the RPC Proxy Server and Authentication Method, Internal Mail Server FQDN, and Mutual Authentication Principal Name. In some of the tests, you need to select the check box to Ignore Trusts for SSL, and finally, you need to select the check box stating that you understand that you will need to provide credentials that are working and acknowledge that you are an administrator of that domain.

Running a test from an external SMTP source (as Figure 1 shows) is as simple as providing an email address, but it can provide a wealth of information for troubleshooting. This test will resolve the MX record and hostname, return the IP address to the email server, test the SMTP port, and try to send a test message to the recipient. Finally, it will test to see if the mail server is an open relay.

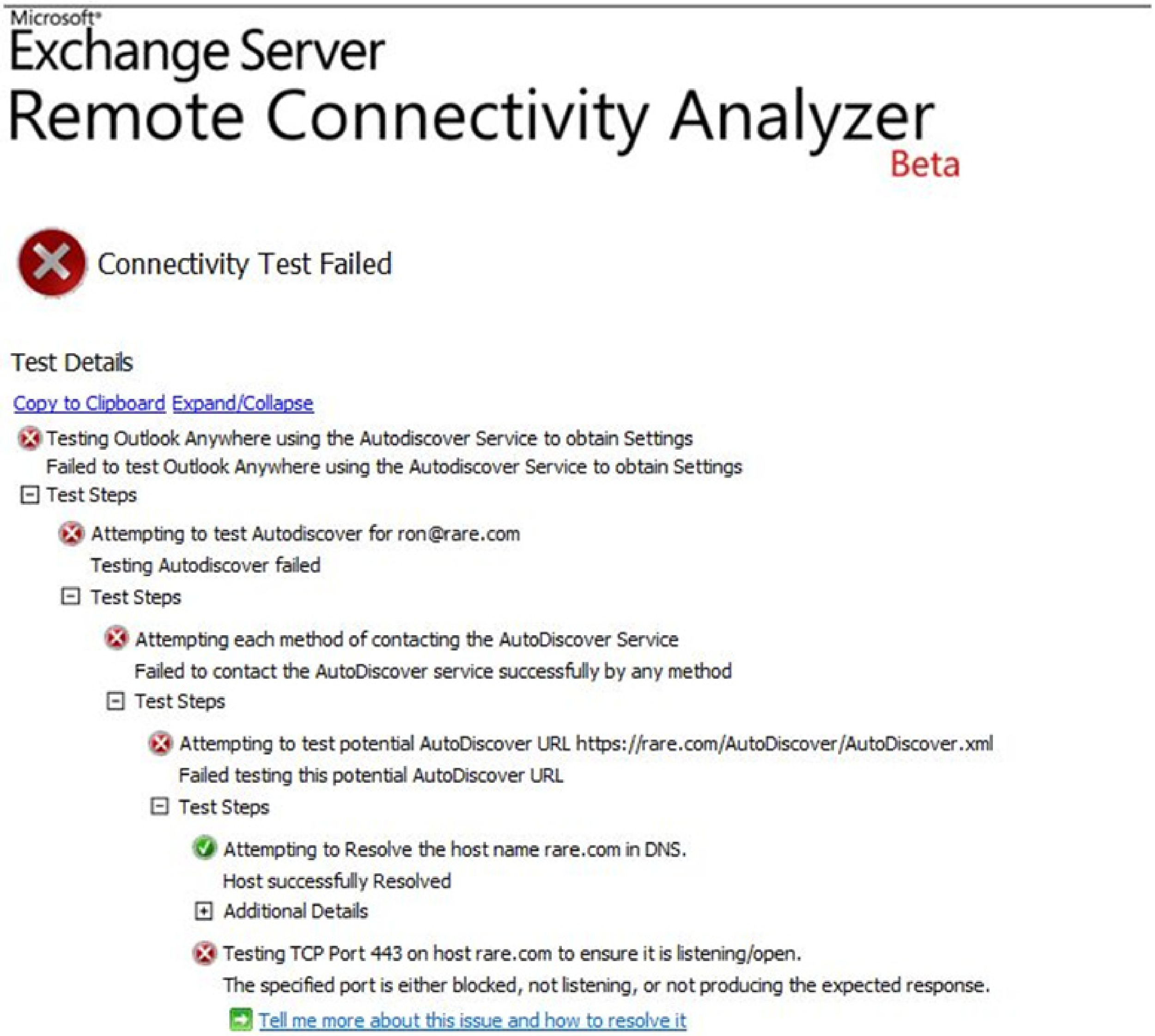


```
✓ Testing Inbound SMTP Mail flow for domain rb@cliptraining.com
  Inbound SMTP mail flow was verified successfully.
⊟ Test Steps

    ✓ Attempting to retrieve DNS MX records for domain cliptraining.com
      Successfully retrieved one or more MX records from DNS
    ⊟ Additional Details
      MX Records Host mx.fusemail.net, Preference 0

    ✓ Testing Mail Exchanger mx.fusemail.net.
      This Mail Exchanger was tested successfully.
    ⊟ Test Steps

        ✓ Attempting to Resolve the host name mx.fusemail.net in DNS.
          Host successfully Resolved
        ⊟ Additional Details
          IP(s) returned: 208.70.128.213

        ✓ Testing TCP Port 25 on host mx.fusemail.net to ensure it is listening/open.
          The port was opened successfully.
        ⊟ Additional Details
          Banner Received: 220 smtp-gw79.mailanyone.net core6 MailAnyone incSMTP bhsmtp ready.

        ✓ Attempting to send test email message to rb@cliptraining.com using MX mx.fusemail.net.
          The test message was delivered successfully.

        ✓ Testing the MX mx.fusemail.net for open relay by trying to relay to user Admin@TestExchangeConnectivity.com
          Open Relay test passed. This mx is not an open relay
        ⊟ Additional Details
          The open relay test message delivery failed (a good thing).
          The exception detail is:
          Exception Details:
          Message: Mailbox unavailable. The server response was: Email Address was not found. (ref 0)
          Type: System.Net.Mail.SmtpFailedRecipientException
          Stack Trace:
          at System.Net.Mail.SmtpTransport.SendMail(MailAddress sender, MailAddressCollection recipients, String
          deliveryNotify, SmtpFailedRecipientException& exception)
          at System.Net.Mail.SmtpClient.Send(MailMessage message)
          at Microsoft.Exchange.Tools.ExRca.Tests.SmtpOpenRelayTest.PerformTestReally()
```

Figure 1: Inbound SMTP email test results.

The Information You Need

ExRCA provides the Exchange administrator with precise points of success and failure (see Figure 2) and even provides links that open right to Microsoft's TechNet site for resolving any failure issues.



Connectivity Test Failed

Test Details

Copy to Clipboard Expand/Collapse

```
☒ Testing Outlook Anywhere using the Autodiscover Service to obtain Settings
  Failed to test Outlook Anywhere using the Autodiscover Service to obtain Settings
⊟ Test Steps

    ☒ Attempting to test Autodiscover for ron@rare.com
      Testing Autodiscover failed
    ⊟ Test Steps

        ☒ Attempting each method of contacting the AutoDiscover Service
          Failed to contact the AutoDiscover service successfully by any method
        ⊟ Test Steps

            ☒ Attempting to test potential AutoDiscover URL https://rare.com/AutoDiscover/AutoDiscover.xml
              Failed testing this potential AutoDiscover URL
            ⊟ Test Steps

                ✓ Attempting to Resolve the host name rare.com in DNS.
                  Host successfully Resolved
                ⊞ Additional Details

                ☒ Testing TCP Port 443 on host rare.com to ensure it is listening/open.
                  The specified port is either blocked, not listening, or not producing the expected response.
                  Tell me more about this issue and how to resolve it
```

Figure 2: Outlook Anywhere test failure with link to more information.

Ron Barrett is the founder of RARE-TECH, an IT training and consulting company. He has been a technology professional for more than a decade, working for several major financial firms and dotcoms. Ron is a specialist in network infrastructure, security, and IT management. He is co-author of The Administrator's Guide to Microsoft Office 2007 Servers, How to Cheat at Administering Office Communications Server 2007, and has been a contributor for several other books on Windows administration. Along with book writing, Ron has contributed to several industry magazines such as Redmond and Windows IT Pro and was featured in the book Tricks of the Windows Vista Masters. He has worked for Microsoft writing research and analysis papers for Windows Server 2008, Windows HPC, and PerformancePoint Server 2007. Beyond writing, Ron has spoken at several technology conferences for CPAmerica and the AICPA as well as TECHMENTOR NYC.

Be sure to catch Ron's daily blog on Network World's Microsoft subnet at http://www.networkworld.com/community/barrett.

Copyright Statement

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.

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. ◆