Net Admin Weekly
59,000 Subscribers Worldwide
September 4, 2002
Issue #7

Feature

Q & A

Security Advisories

News Headlines & Resources

Download of the Week

Feature

The Ten Commandments of Troubleshooting

to top

In part 1 of "The Ten Commandments of Troubleshooting", we went over some techniques you could use to solve problems faster and more efficiently. Those first five commandments brought in a lot of praise from you readers. For that, I say "Thank You"! Today I complete the series by presenting the last five Commandments of Troubleshooting.

6: Don't overlook the obvious.

An unaware troubleshooter could spent hours attempting to "fix" a computer that "can't get on the Internet," uninstalling and reinstalling its TCP/IP stack, reconfiguring its DNS settings, or releasing and renewing its DHCP lease, only to overlook the most obvious answer: the file was not found because the file is not there. Sometimes it's really that simple.

On the other hand, if you try to reproduce the problem at another machine and find that you can access the site from there, you know there is most likely a problem with the first machine's configuration. Then it's time to focus your investigation on that particular computer. Perhaps the first thing to check is whether you can access other websites or it's only this one that's giving you problems.

If our original complainant/user was right and "the Internet isn't working," or rather, the web doesn't seem to be working – but other Internet applications like email are – our next step would be to determine whether we actually have a connectivity problem or just a name resolution problem. To do that, we can try connecting to a website using its IP address.

If you type http://www.microsoft.com into the browser's address box and get nothing, but the Microsoft homepage comes up fine when you type in http://207.46.131.30, you know the "friendly" name is not being translated into the format the computer understands, the IP address. Since you know DNS is the service that performs this resolution of fully qualified domain names (hierarchical "dotted" names like URLs), at this point we can be fairly certain that there is either a problem with the computer's DNS settings or (if other computers that use the same DNS server are having the same problem) with the DNS server itself.

7: Try the easy way first.

Most of us have heard it said of someone, usually in a whispered voice accompanied by a frown, "he always has to do things the hard way." The same critics may then turn their disapproval on someone else with the indictment that "he always takes the easy way out."

Did you ever wonder how both of those philosophies could be wrong? Or was the latter criticism tinged with a hint of jealousy? In troubleshooting connectivity problems, it certainly pays to at least try the easy way first. How many times have you been able to correct a problem simply by rebooting the machine? It may not work, but it never hurts to try simple solutions before implementing the more complex ones.

In fact, you should make it a practice to always evaluate all the possible solutions to a problem, and then try those that are easiest, quickest, and/or least expensive, and leaving the difficult, time-consuming and costly fixes as last-resort alternatives. If you have two machines that won't "talk" to one another on the network, you would not be advised to first try rewiring the building just in case it's a cable problem.

8: Document what you do.

It may seem like a lot to ask, after you've endured all that blood, sweat and tears to finally get the problem solved and get the network back up and running, but documenting your troubleshooting activities is vitally important. Putting down on paper the steps you go through, as you perform them, serves several purposes.

First, it helps you to stay organized and perform those steps methodically. If you're writing it down, you're less likely to skip steps, because it's all there in front of you, in visual form. You don't have to wonder "did I test that cable segment?" or "did I check the default gateway setting?"

Documenting your actions also provides a valuable record if you end up having to call in an outside "consult" or otherwise request someone else's assistance with the problem. Time, and often money, will be saved if you can provide detailed information about what you've tried, how you proceeded, and what the results were.

Unfortunately, in the corporate world you may also sometimes find your documentation necessary for "CYA" purposes. A network outage that lasts for a significant amount of time can, in some businesses, cause a huge financial loss, even threaten the company's position in the industry or – in extreme cases – put a business out of business.

Luckily the consequences aren't usually that dire, but you'd better believe many firms are heavily dependent on their network communications. If your job description makes you responsible for the welfare of the network, you're less likely to get caught in the scapegoat-hunting process if you have detailed documentation of your efforts to address the problem.

Finally, you should document the troubleshooting and problem resolution process for a very practical reason: history tends to repeat itself and human memory is imperfect. As you wipe the perspiration off your brow and breathe a silent sigh of relief at having finally tracked down and solved your connectivity problem, you may think that there is no way you will ever, ever forget what you did to fix it – not after going through all that agony. But a year later, when the same thing occurs again, it's likely you'll remember only, "This happened before and I fixed it -- somehow." The details tend to get lost – unless you write them down.

One last caveat on documentation: it's great to have a nice, neatly typed (and maybe even illustrated) troubleshooting log, but if you do your record keeping on the computer instead of manually, it's a good idea not only to back it up to tape, floppy, writable CD, or other media, but also

to print out a hard copy. It should be a given, but sometimes folks forget that when the computers go down, computerized documents may be inaccessible.

9: Practice the art of patience.

Patience is a virtue, so hurry up and develop this characteristic! Whether or not you aspire to be virtuous, patience is an asset in any sort of investigative work, and that's what network troubleshooting is.

This means being patient enough to go over each configuration setting in each machine, to test each cable segment, to try one solution and, if it doesn't work, to keep trying new ideas until one does work. Finding the source of a connectivity problem is often like looking for needles in haystacks; you must have a "system" and you must implement it methodically.

This also requires that you be patient with users, even when they seem to be the bane of your existence. Remember users are also one of the big reasons for your job's existence – you're there to support them, as well as the computers to which they're "attached."

Finally, you must be patient with yourself. It's easy to get exasperated when the network is down, the pressure is on, and nothing you do seems to help (or your best efforts seem to make the problem worse). If users are one of the reasons your expertise is needed, there's an even bigger reason: problems. A network that ran smoothly all the time, one in which the server never mysteriously went offline and computers never suddenly stopped "talking" to one another for no apparent reason and communications never got strangely garbled would be a network with no need for an administrator.

Trouble is what you live for – or should be! A good network administrator doesn't see problems as something to fear or curse, but as challenges and learning experiences. Continuous learning is what the job is all about, and you'd better love learning new things if you intend to lead a happy life as an IT professional. There's one thing that's a certainty in this business: you can never learn it all. And if you did, there would be a brand new and different technology ready to take the place of the one you'd just mastered.

10: Seek help from others.

Network admin types tend to have some common personal characteristics: they're bright, they're self-starters, they're just a bit (okay, maybe more than just a bit) more comfortable when they're in control, and they've got a lot of pride.

Taking pride in doing a good job is an admirable trait, but that pride can also make it hard for you to admit that a problem has you "bumfuzzled," as my grandmother used to say (meaning you've tried everything you can think of and the answer – sometimes even the question – still eludes you). Don't be so proud that you can't bring yourself, when necessary, to ask for help.

Asking for help after you've exhausted all your ideas is not an admission of defeat, it's just a step in the troubleshooting process. Using your resources is smart, and those resources include product documentation, books, websites, newsgroups, mailing lists, and other working professionals in the field.

Remember that the term "networking" has another meaning: getting acquainted with people in your profession who can be beneficial to your career. Someone you know may have struggled with the very same problem that is vexing you now. Why reinvent the wheel? Ask for help.

Most people are flattered to be asked to share their hard-earned knowledge – as long as you don't abuse the privilege. Calling good old George every couple of months with a quick question is likely to make him feel that you respect his expertise. Calling him every week with a complicated problem that you need solved "right away" will make him feel that you don't respect his privacy.

How do you find knowledgeable, experienced IT pros whose brains you can pick when you have a problem? There are many ways to make contacts: attend seminars, join Internet discussion groups devoted to networking topics, stay in touch with classmates and instructors from the training courses you attend.

There is a corollary to this commandment. Be available to share your own expertise with others when they need your help. The best networking methods, after all, use two-way communications.

Conclusion

It takes more than just networking knowledge to make a living in this business. You need to take that knowledge and apply it. When it comes to troubleshooting, the best way to apply that knowledge is to use a methodical, measured approach. If you follow the ten laws of troubleshooting you'll solve your problems faster than the next guy, who just keeps clicking, hoping to find the right combination of clicks.

This week's feature article by
Deb Shinder
Net Admin Weekly Author

Q & A

Unable to Create New DNS Zone on Windows 2000 DNS Server

to top

Question:

Hey Dr. Tom,
I'm having some troubles with configuring a DNS zone for my organization. Our first level domain name is militaryarts.com. I want to create subdomains names com1.militaryarts.com, com2.militaryarts.com and com3.miltaryarts.com. The "com" reflects the command structure of

our organization. However, when I try to create the Standard primary zone for any of these domains on my Windows 2000 DNS server, the attempt fails. What can I do to fix this? Thanks! --J. Head

Answer:

Hey J! Great question. I bet if you created a domain like west.brainbuzz.com it would work fine. So what's the problem? The problem is that when you create standard domains, the zone information is stored in a zone file on the hard disk and the name of the file is based on the domain name. The files system doesn't allow you to use the words: AUX, COM1-4, LPT1-3, CON, NUL, PRN. When the Windows 2000 New Zone Wizard tries to create the file, it gets stopped in it tracks. However, there is a workaround that will allow you to create your domain, but use a different file name for the standard DNS zone file. The DNSCMD command gives you this flexibility for example:

DNSCMD /zoneadd com1.militaryarts.com /primary /file com1militaryarts.com.dns

The /zoneadd switch indicates that you want to create a new zone. The /primary switch indicates that this is a standard primary zone (with its information stored in a file). The /file command allows you to input a file name of your choice.

Simple Steps to Help Bulletproof Win2K

to top

Question:

Hey Sgt. Deb,
Okay, I've been listening to all the security experts who say that Windows 9x/ME is an inherently insecure operating system, and I've upgraded to Windows 2000 (yeah, I know it's already obsolete and XP is Microsoft's latest and greatest, but I tend to move slowly, okay?) but I'm wondering if all my security problems are now solved, or are there things I need to do to make sure my Windows 2000 computer is as secure as it can be? -Slow Mover.

Answer: Dear SM,

You've taken an important step, security-wise, by upgrading to an NT-based operating system. Windows NT, 2000, and XP are built on a kernel (the core operating system code) that's very different from that of the 9x family. Because they're designed for the corporate environment, they include the features most valued by business customers, and security is definitely a top priority in today's business world. However, just because W2K includes more security features, that doesn't mean you're taking advantage of them just because you've installed the OS. To make your W2K (or XP) machine really secure, you should be sure to address the following issues:

1) Make sure you've formatted all partitions in NTFS. While W2K and XP will support FAT partitions, you lose many of the security features such as file level permissions and EFS encryption when you use FAT.

2) Disable services you don't need (for example, the web server service if you don't intend to use the machine as a web server) and unneeded user accounts, such as the built in Guest account.

3) Set strong passwords, especially on administrative accounts. This means passwords of at least 8 characters in length that use a combination of alpha (upper and lower case), numeric, and symbol characters, that are easy for the user to remember but hard for others to guess (not words that are in the dictionary). Also, change these passwords on a regular basis.

4) Use password policies (set through Group Policy) to enforce strong password rules.

5) Change the name of the built in "master" administrator account and create a "decoy" account named Administrator that has minimal permissions.

6) Remove all unnecessary shares; disable file and print sharing completely if you don't need to share resources on the machine with anyone across the network.

7) Set NTFS (file level) permissions on files and folders in addition to share permissions on shared resources. Be aware that the default share and NTFS permissions give the Everyone group full control; this should usually be changed on each resource.

8) Set an account lockout policy (in Group Policy) that will lock out a user account after a specified number of incorrect password entries.

9) Use Group Policy to set up security auditing so you will be aware of failed or successful logon attempts and other security events.

10) Be sure to install and update antivirus software and apply the latest security fixes and service packs.

Security Advisories

Buffer Overrun in TSAC Client ActiveX Control

to top

If you use the Terminal Services Advanced Client (TSAC), you'll want to get this one right away. There's a buffer overrun vulnerability in the TSAC ActiveX control that can allow an attacker to run commands in the context of the logged on user. Read more about it and get the fix here.

Read more...

Apache Flaw Leaves Server Wide Open

to top

Heads up if you're running Apache version 2.0 on Windows, OS/2, or Netware. There is a vulnerability that allows an attacker to damage the server and reveal sensitive data stored on the server. UNIX platforms are unaffected by the problem. For more info and a fix, check out the link.

Read more...

IDS in the Trenches

to top

Intrusion Detection Systems provide a powerful way to keep tabs on the goings on in the perimeter. But are those IDSs as powerful and useful as their vendors claim? This article brings together five InfoSec experts in a roundtable discussion. Definitely worth a read!

Read more...

News Headlines and Resources

How to Really Screw Up a Linux Installation

to top

Linux can be a lot of fun, *if* you can get the darned thing installed! Linux maestros don't have the benefit of the finely crafted installation routines Windows users have at their fingertips everyday. In this article, Mary Robinson shares with you one reliable method to bollix up a Linux install.

Read more...

The Miraculous WMI Scriptomatic Tool!

to top

Have you ever wanted to automate a process that takes you hours to accomplish by hand? Sure you have! But you just don't have the time right now to sit down and learn WMI scripting. The WMI Scriptomatic Tool might be just what you're looking for! Read about and download this cool tool here.

Read more...

Break the Office Stranglehold with Open Office File Types

to top

What allows Microsoft Office to remain the de facto standard for Office Suites? It's the fact that almost everyone has used Office and they're locked into the Office File types. Open Office uses XML and the specs are published. This article discusses how the Open Office file format could be the wave of the future.

Read more...

Download .NET Server Release Candidate 1

to top

You'll be hearing a lot more about Windows .NET in the coming months. They've renamed it to Windows .NET Server 2003, which means it probably won't be out by the end of this year (although you never know). The change gives you more time to get ahead of the curve and learn about .NET Server. You can order the Windows .NET CD or download the operating system here.

Read more...

DNS Poisoning and Domain Hijacking

to top

During my years as trainer and consultant, I've consistently found that DNS is the least understood subject among network admins. Things are getting better! Here's a great article on a major issue in DNS security: DNS cache poisoning and domain hijacking. I guarantee you'll like this one!

Read more...

Cool Tip: Saving and Opening to and from FTP Sites

to top

We've been working with Microsoft Office for years, and never knew about this one! Did you know you could save and open Office documents to and from an FTP site? If not, head on over to this Q article and get the specifics.

Read more...

Support Webcast: Deploying a Secure Windows .NET 2003 Network Infrastructure, Part 1

to top

This Support WebCast introduces Windows .NET networking components and discusses how they can be used to successfully enable secure network access. This promises to be a very interesting talk, as Windows .NET 2003 introduces many new networking enhancements.

Read more...

Download of the Week

Diskeeper Lite 7.0

to top

Sure, you can use the built-in defragger in Windows 2000/XP, but why deal with its poor performance? Even though the built-in defragger is based on Diskeeper technology, its not Diskeeper 7.0. Executive software has a cool FREEWARE version of Diskeeper 7.0 that beats the pants off the built-in version. It's much faster! Like the built-in version, it only does manual defrags; you'll need the full version to schedule a defrag.

Read more...

Free Cramsession IT Newsletters - Choose Your Topics!

H = HTML Format **T** = Text Format

H	T		H	T		H	T	
☐	☐	A+ Weekly	•	☐	Exam Tips 'N Tricks	☐	•	.NET Insider
☐	•	ByteBack!	☐	•	IT Career Tips	•	☐	Script Shots
☐	☐	Cisco Insider	•	☐	Linux News	☐	☐	Security Insider