DNS Active Directory Rescue Planning

Contributed by David Noel-Davies

A few years ago (and them some!), I received my scuba certification. The most valuable lesson in that class: Stop, think, and do a little planning before you jump into the water. Failure to heed this warning could cause the bends, or possibly death. Our instructor's mantra: Plan your dive; dive your plan.The same philosophy applies to network administrators performing large upgrades or implementing a new technology that could affect production. Too often I've seen otherwise competent technologists paint themselves into a corner because they lack a clearly defined implementation roadmap. Instead, they simply pop in the upgrade CD-ROM, double-click setup.exe, and walk through the wizard. This approach almost always leads to disaster.

This happened recently to an administrator acquaintance of mine who was trying to upgrade his Windows NT 4.0 domain to Active Directory (AD) and Windows Server 2003. He was new to network administration and didn't realize the importance of having a well-thought-out plan. Eventually, he asked for help, but by then host names weren't resolving correctly, Group Policy didn't work, and the event logs were full of errors. We talked through the issues on an online forum, via email, and eventually over the phone. From what he described, it appeared that DNS and AD weren't communicating with each other. Here I'll talk about what we did to fix the problem (during a weekend, mind you), AD-DNS Chaos

We found these AD and DNS problems (among other, less severe ones):

- Domain controllers (DCs) didn't point to a DNS server.
- AD DNS Resource Records (RRs)—_msdcs, _sites, _tcp , and _udp— were missing.
- DNS wasn't set to accept dynamic updates.
- Clients pointed to the ISP's DNS server instead of an internal DNS server. The administrator didn't understand the importance of DNS in an AD environment. No DNS means no AD. Finding that the AD DNS entries were blank provided me a great opportunity to explain to the admin the importance of DNS and how it worked. After we configured the correct DNS settings on each DC, we moved on to dealing with the next problem: the missing RRs.When I looked in the DNS zone for the domain, it immediately didn't look right. I couldn't place my finger on the problem at first until I went back to my test domain and compared mine with the administrator's. Then the problem stuck out like a sore thumb: His domain didn't have the needed RRs! This adventure was getting more exciting by the minute. I had him reboot the DC, fully expecting the missing information to reappear. But rebooting didn't restore the absent RRs, so my next step was to have the admin cycle the Netlogon service by entering the following at the command line: net stop netlogon net start netlogon Still no RRs. Eventually, we turned to Microsoft Help and Support and found the article "How to reinstall a dynamic DNS Active Directory integrated zone" (http://support.microsoft.com/?kbid=294328). We followed the steps in that article to totally remove DNS and reinstall it fresh. The process was straightforward and fixed the problem.More DNS Troubles

The third issue we discovered—that DNS wasn't set to accept dynamic updates—could also explain why some of the PCs weren't resolving IP addresses correctly. The PCs had entries in DNS, yet those entries weren't being updated when the PCs' IP addresses changed via DHCP. The solution was simply to configure the clients to allow DNS dynamic updates. The last problem we found is something that I see a lot when companies migrate from NT to AD. In NT, there usually wasn't a reason to use DNS to resolve host names; we just used WINS to resolve NetBIOS names. DNS then was left to resolve Internet names for browsing in Internet explorer (IE). This process worked well in an NT environment, but it's a paradigm that needs to change when you move to AD. Client computers need their DNS to point to an internal DNS server so that AD services such as Group Policy work correctly. In Windows 200x, you live and die by DNS.Situation Normal

It took a few days for us to straighten out all the glitches in the administrator's network, but in the end the network was spinning like a top. Although you can't foresee every network trouble that could occur when you perform a major OS upgrade, in my experience I've learned that having a carefully considered upgrade plan in place—and following that plan—go a long way toward avoiding the type of snafus that plagued my network administrator colleague.