

Every IT person has some interaction with a DNS server, even if it is not managing it. Most DNS servers, certainly the majority are sitting in some closet or rack somewhere dutifully running and collecting dust. Like a certain battery operated bunny, these services just keep on running. The durability of DNS (Domain Name System, that is) is a testimony of just how well it was designed. DNS serves every single user of the Internet consistently, day-in and day-out. What DNS does and how well it does it is nothing short of an engineering miracle simple, elegant, scalable - truly amazing. How often do you think about your DNS server? Here is my plan for how to keep your relationship with your DNS server alive and well.

1. Check your system logs to make sure there are no impending hardware failures on the horizon. For example, be sure you have SMART enabled to check your systems hard disks and make sure that you can receive the SMART alerts should they occur. You should also review your logs for any other errors such unexpected reboots that you may have missed.
2. Monitoring, you should really think about monitoring your DNS server. Is it up? Is it responsive? Is it giving the right answers? Can those who need to access it connect?
3. Don't confuse things. Don't run a recursive name server that is also the start of authority for a DNS zone. You really, and I mean really, need to separate these functions to different servers. If you don't you are opening your zone to a very high level of risk.
4. Check your DNS server version. Make sure you are running the latest version of you DNS server software. This is imperative.
5. OS updates are critical as well. Make sure you keep your system up-to-date!
6. Run only DNS on your DNS server. You can run other software but you then have to be concerned that periodic (required) updates to your DNS software could impact other parts of that server. So the less you are running on that server the less risk. Just an idea.
7. Never have only one DNS server. You absolutely need two resolver servers and two SOA servers, at a minimum.
8. Try to have your SOA DNS servers on different networks with different paths to the Internet. If you do this and one of your networks goes down people will still be able to resolve your zone.
9. Backups. Right now - go and do a dry run to restore your DNS server. If you are thinking, "boy, how do I do that?" you should panic. You don't want to ask that question when it really fails. Get your ducks in a row right now.
10. Replace older hardware. The nature of hardware is that it fails. Proactively plan for replacement of your DNS server.

So please take a few minutes and at least think through each of these issues. DNS will always be an attack target. DNSstuff can help with robust tools and proactive alerts that verify configuration and assist with troubleshooting and resolution. Having DNSstuff's web application at your fingertips is a must for IT professionals.