

## Enterprises Are Not Taking DNS Seriously

DNS (Domain Name Service) is the key technology in modern IT infrastructures - without it, your business stops. Every single application now relies on DNS in some way or another.

Want to send an email? Your email program uses DNS to find the IP address of your mail server so it can send the email.

Want to print something? Your PC will use DNS to find the IP address of the printer.

Want to access your company's corporate database? Your application will use DNS to find the IP address of the database server.

DNS acts as a big electronic phonebook that catalogues all the IP addresses of the servers and printers on your network. Without it your PC will struggle to access these other systems.

So when I visit sites that are still running DNS on an ageing Windows NT server under someone's desk, I am horrified.

In many cases, DNS servers have been deployed in response to a specific requirement - someone needed a DNS server in order to implement a proxy server or a specific application required a DNS server. But as more applications and services are deployed, the DNS infrastructure is often the last thing that is considered. DNS servers and domains have often been deployed without an overall strategy, leading to an unstructured, non-resilient, and badly configured mess.

Install an Active Directory Domain Controller, and it will attempt to resolve the AD domain name in DNS. If you don't have a DNS server on your network, or it can't contact one, it will automatically install one on the DC. "Great" you might think, "it's doing all the hard work for me", but this is implementing DNS in an ad-hoc approach that might not best suit the business in the long term. For instance, the DC you just installed might be in a remote location or on a network segment that is not resilient. The fact that DNS is running on a DC means that it is not on dedicated hardware, so other applications may impact performance or the availability of the server. Installation of critical Microsoft security updates is crucial but in many cases requires a reboot that will affect the availability of the DNS service running on that DC.

When your infrastructure has grown to rely on DNS servers co-hosted on Microsoft servers, it soon becomes apparent that applying Microsoft security updates and service packs impacts the availability of not just that single DC, but every application that relies on DNS. Reboots have to be meticulously planned in order to determine which applications will be affected, and to ensure that those applications can reach backup DNS servers. Without adequate planning of the DNS infrastructure, you start to discover incorrectly configured application servers that have no secondary or tertiary DNS servers configured, or have servers configured that no longer run a DNS service. Furthermore, without any monitoring, you may discover servers where the DNS service has stopped or crashed.

These misconfigured systems only become visible when a DNS server fails or is rebooted for maintenance, and the impact can range from a minor inconvenience (the CEO can't get his email) to disastrous (a bank's trading floor suddenly incapacitated for 15 minutes while the stock market is falling).

In order to prevent these issues from impacting the availability of the DNS service, some larger enterprises are starting to take their DNS infrastructures seriously by taking a holistic approach. This involves making an individual or team responsible for the entire DNS infrastructure and deploying dedicated DNS server appliances that are managed by that team. Taking this approach enables the "DNS team" to arbitrate between different projects' DNS requirements and ensure that a structured approach is taken to the configuration of new DNS domains and servers. Quite often, companies will deploy an IP Address Management ([IPAM](#)) product to help them manage the assignment of IP addresses and automate updates to the DNS environment.

Unfortunately these companies are in the minority rather than the majority. Too often DNS is seen as a service that belongs neither with the networks team nor the server nor application teams, and so often "falls between the cracks". For such an important service, it simply isn't good enough.

I believe that taking a holistic approach to your DNS infrastructure will help improve application availability:

- Nominate a person or team who is responsible for the DNS and can support and co-ordinate DNS requirements from different projects
- Use dedicated servers or appliances to reduce outages due to maintenance

- Place DNS servers in your data centres or at the core of your network (e.g. make sure they are "well connected") so everyone knows which servers to use

- Ensure all your WAN links are resilient

- o If you have locations where this is not possible, you may need to consider installing a local DNS server

- Ensure the server/appliance hardware you install is resilient

- o RAID 1 disk mirroring or solid state storage

- o Dual PSU's (connected to different power feeds)

- o UPS

- Ensure the server has out-of-band management capabilities to assist with upgrades and troubleshooting (RiLO, DRAC etc.)

- Monitor the DNS servers to ensure they are operating within normal parameters

- o Graph CPU and memory utilization, network throughput, DNS availability and DNS queries per second

Following this approach will enable you to reduce DNS outages to a minimum and provide a higher level of service to your business.

## About the Author

Article written by Paul Roberts, Professional Services Manager at n3k.

n3k deliver [DNS management](#) and supply DNS, [DHCP Appliances](#), as well as training, consultation and reporting on all matters to do with DNS. Visit <http://www.n3k.co.uk> for more information.

Source: <http://www.zogol.com>