

THE CHALLENGES WITH DNS

DNS is absolutely mission critical. DNS runs the Internet. If your DNS isn't working, you lose your ability to communicate with the outside world through the Internet, and customers lose their ability to contact you.

Managing and maintaining DNS can present a challenge for any sized organization. For a company to create manage and maintain their own DNS means using expensive IT professionals to develop customized network functions. These customized solutions require the purchase of expensive hardware, software and many hours of integration and maintenance to develop and sustain.

Furthermore, the full complexities of network functions such as DNS are often not fully understood by many IT professionals, resulting in sub-optimal solutions with numerous security flaws. As DNS is the main point of entry between the internal network and the outside world, DNS is also one of the first areas hackers probe for access.

Organizations recognizing the importance of DNS want greater control over their DNS system, especially to address security concerns. These organizations must use software to run DNS, and the software is usually either a version of BIND running on a UNIX server, or Microsoft's DNS Server running on a Windows box.

DNS Concerns: Administration is Time Consuming and Costly

The main shortcoming of DNS is its administration and management. For many IT professionals, administrating DNS and BIND is a time consuming task. As an organization grows, maintaining DNS becomes extremely difficult and time consuming, and the chances for mission critical errors increase considerably. If a technician types one dot out of place when entering a DNS address, the visitors looking to reach that Web site may be routed to an address that doesn't exist.

BIND uses a pure syntax based administration, requiring personnel to type in extremely complex syntax commands with 100% accuracy. Not only is BIND non-intuitive, it's tedious as well, requiring more administration effort each time your site changes. Administrating zones is incredibly complex and more confusing the larger your site is. For each zone, BIND administrators must configure both a forward and reverse lookup. This means that if you say, "IP address 209.167.177.34 equals www.bluecatnetworks.com", you have to do the reverse lookup as well, which means typing in the address backwards (wwwbluecatnetworks.com equals 209.167.177.34).

Bottom line, administrating DNS in BIND is a syntax nightmare as there is no room for error. Even worse, there is no data checking function to find errors that have been made. Typically, as an organization's web presence expands, top administrators rather than less experienced IT staff find themselves spending a considerable amount of time maintaining DNS.

With the expansion of web services, organizations need a solution that is more cost effective and easier to manage, and that will eliminate the risk of critical errors inherent to DNS administration.

DNS Concerns: Security and Updates

DNS is the main port of entry between the network and the outside world, and as such, it is often the first point of attack for hackers. There are a number of steps that should be addressed to mitigate security concerns around DNS.

Single Purpose DNS Server

It is a good practice to run DNS servers that are dedicated to a single purpose. By limiting the number of applications running on your DNS server, you are limiting the possible ways a hacker may attack it. Every additional application will open ports, increasing potential access to your DNS server. Harden the server and disable daemons that have well known vulnerabilities. Filter out all traffic except traffic from the Internet on port 53, and run DNS on a dedicated server.

Patches and Latest Builds

It is important to stay up to date with the latest releases of BIND. All older names servers have widely known vulnerabilities that can be exploited, such as susceptibility to denial of service attacks, and the ability to remotely execute code. DNS must constantly be updated and upgraded against known security vulnerabilities. As neither BIND nor Microsoft offer automatic updates, IT staff must spend considerable time ensuring their versions of DNS protocols are up to date. Administrators

must constantly monitor for security upgrades and patches, and then spend time to manually upgrade their systems. Administrators need to ensure their DNS is the most current and secure version, and ideally have an efficient, automated way of receiving these security updates.

Split Internal & External DNS

It is a good practice to run separate internal and external DNS servers. Typically an organization's internal network is populated with hosts that hold sensitive data. By having separate DNS servers for the internal network, you can keep the IP addresses and names of sensitive internal hosts invisible from the Internet.

Disable Recursion

Recursion should be disabled on external DNS servers for two reasons:

- 1) Recursive queries take a longer time to resolve. The DNS server's resources are tied up for longer periods of time. This can be a basis of DoS attacks that cripple a DNS server.
- 2) A malicious hacker can use recursive queries to perform DNS spoofing and poison the cache on the target DNS server. This may cause sensitive email to be misdirected, or web browsers to be redirected to the wrong web sites.

When creating DNS configurations, disabling recursion is often overlooked. Ideally this service should be disabled by default.

Diverse Locations for DNS Servers

As demonstrated by Microsoft's web service outage in January 2001, an incorrectly configured DNS architecture can lead to serious consequences. The DoS attack was possible because all of their servers were located in the same physical location and on a network behind a single router. Obviously a good design should locate DNS servers on different network segments so that failure or a DoS attack on any one segment would not render your DNS inaccessible.

Restrict Zone Transfers

This is important for 2 reasons:

- 1) By not restricting zone transfers, DNS servers are more vulnerable to DoS attacks. An attack can create a script that will repeatedly perform zone transfers from the target server, causing the resources and bandwidth to be tied up.
- 2) By performing a zone transfer, an attacker can quickly and easily obtain a map of the target network. This data holds the name and IP address of every host on the network, providing invaluable information to a malicious hacker.

By default, zone transfers should be allowed to an explicit list of hosts only.

Authenticate Zone Transfers

The use of transaction signatures (TSIG) ensures that a slave server can verify the authenticity of the zone data through the use of cryptography based on a pre-shared key. This will prevent the slave being updated with fraudulent information.

Restrict Dynamic Updates

Supporting Dynamic Updates may open up vulnerability on improperly configured DNS servers. To avoid this, you must restrict updates only from trusted IP addresses or subnets. Some DNS administrators use the 'catch all' approach to open up dynamic updates to all zones. This is a risky practice that opens up the zone to malicious updates.

Hide the BIND Version

By default, BIND will respond to queries regarding its version. With this information, a hacker will know which exploits to run against the DNS server. This feature should be disabled by when configuring DNS.

Firewall Protection

IANA has assigned TCP and UDP ports 53 to DNS queries. When running a single purpose DNS server, the firewall rules should be written to only allow traffic to port 53 bound for the DNS server. Even better, an onboard firewall will provide another layer of security.

File Backup

Backup all DNS server configuration files. This prepares you for incidents where a hacker may have broken through your defenses and corrupted data on your DNS server. A DNS Management Software product can help. Besides taking the drudgery out of manually configuring BIND, the Management Software will ensure there is a current backup of your configuration data.

Hardware Spares

No piece of hardware is infallible. There will come a time when your DNS server hardware physically fails. This may not specifically be a security issue; it is a factor that will affect the availability of your name server. Having a spare piece of hardware is a great insurance policy.

Adonis DNS Server: #1 Secure DNS Server on the market



Adonis is a complete dedicated DNS administration solution that integrates powerful Java technology into a simple, low-cost network solution. The Adonis DNS Management Server was designed to simplify designing, implementing and maintaining a domain name service

Why: DNS is Mission Critical:

DNS runs the internet.

Without it your customers lose the ability to communicate with the outside world through Internet and email.

Challenges with DNS:

Time Consuming & Costly:
The main shortcoming of DNS is administration & management.

Administering DNS in BIND is a syntax nightmare, with no room for error. Even worse, there is no data checking function to find errors that have been made, as a result IT staff find themselves spending a considerable amount of their time maintaining DNS.

DNS is the main point of entry between the network and the outside world, and as such it is often the first point of attack for hackers. DNS must constantly be updated and upgraded against known security vulnerabilities.

Security:

Adonis is your most secure option for a DNS server, employing T-Sig, hardened kernel, True Authentication, 2-way SSL encryption and multiple Digital Certificates (both client - server).

The Adonis DNS Server is ranked as the #1 DNS Server by both [Network Computing Magazine](#) and the [Well Connected Awards](#). No other product comes close to Adonis' simplicity and security.