

# TOP 10

things you  
can do to  
ensure proper  
and secure  
DNS operation.



- ❑ 1 Make sure you are running the latest patches for your dns server software, if not the latest version outright. If there are known security vulnerabilities in your DNS server software, it is a virtual certainty that you will be the victim of an attack or attempted attack.
- ❑ 2 Run BIND 9, it has great security enhancements, features, and capabilities beyond most other DNS servers. For example, BIND 9 supports views, which allow you to serve different records (and entire configurations) for the same zone depending on the client IP; this is useful to create split-horizon DNS or even to do basic geographic based load balancing.
- ❑ 3 Ensure the security basics are covered. Disable zone transfers and anonymous dynamic DNS updates, do not publish data via DNS that you don't need to publish, and disable recursion.
- ❑ 4 Ancillary to #3, if you need to provide recursive DNS to employees, customers, or anyone else, do so on a server that is not responsible for any zones. This is basic security partitioning and simply makes sense in more instances than simply making one server do both jobs.
- ❑ 5 Run multiple dns servers, and possibly different versions of software on each of them if those versions are actively maintained. This will help prevent new bugs in the latest version from disrupting all of your DNS servers.
- ❑ 6 Be certain that DNS servers listed for the domain in your zone match those listed with your domain registrar. Every nameserver listed at your registrar should have a matching record in the zone configuration; it is ok to have more nameservers listed in your zone than at the registrar, but the extra servers will not be used as often as those listed at the registrar.
- ❑ 7 If you use a managed DNS server solution, such as easydns or the built in services of your registrar, see if you can use more than one of them. This will ensure that an outage at one provider doesn't make your entire site unavailable.
- ❑ 8 Do your best to ensure RFC compliance on your servers and within your zones. Non-compliant servers or records can adversely affect people attempting to resolve your domains in the case of an authoritative server, or your customers, employees, or users in the case of a caching non-authoritative server.
- ❑ 9 Ensure that the OS hosting your DNS servers has a strong pseudo-random number generator (PRNG). The PRNG in most modern OSes is sufficiently strong that you don't have to worry, but if you have any older servers it would be worthwhile to test them.
- ❑ 10 Roll out DNSSEC on all of your domains and zones. DNSSEC provides strong cryptographic signing of DNS records, via a chain of trust all the way back to the root, in order to prevent forging of records. DNSSEC will not achieve the security it promises until the TLDs are signed, as well as the root zone, but being prepared ahead of time will not hurt.