

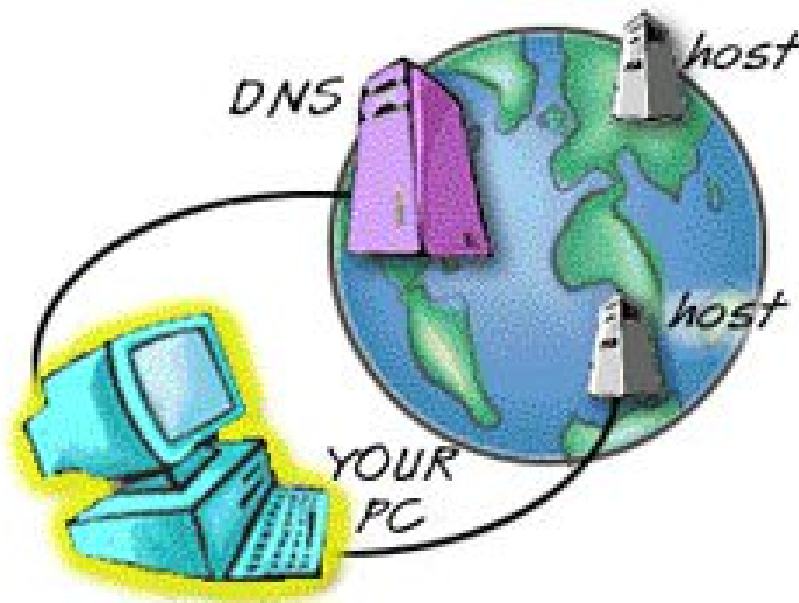
7 issues to avoid when deploying DNS

Domain Name System (DNS) is a known method for combining domain names with IP addresses. It is now a solid set of methods, most of which have worked perfectly, although there are still some cases of malfunction and that is not true.

Cricket Liu

Domain Name System (DNS) is a known method for combining domain names with IP addresses. It is now a fairly solid set of methods, most of which have worked perfectly, although there are still some cases of malfunctioning and that is when the system administrators sort things out. What is wrong.

Here are 7 most common problems - 7 felony against DNS:



1. Using old versions of BIND - All but the current version of BIND 9 (9.3.4-P1 and 9.4.1-P1), there are many serious vulnerabilities. Hackers can exploit this vulnerability to sabotage your servers, invade existing hosts and much more .

2. Put all authenticated name servers on the same subnet - failure of a single device - like a switch or router - or users cannot connect to the Internet when they want to access the website or send mail.

3. Allow recursion of non-authenticated queries - handling recursive queries for clients to display your server, thereby leading to intrusion actions and denial of service attacks.

4. Allow migration zone to non-authenticated secondary servers - a small amount of moving area to arbitrary requestors can harm your server as well as exploits that can be exploited.
5. Disadvantages of using forwarders - many types of servers, such as Microsoft DNS Servers or older BIND servers, are not adequate to counter intrusion acts and have vulnerabilities that can be exploited by many other forms. . Some administrators also allow this server to query servers on the Internet directly without using a forwarder.
6. Setting wrong Start of Authority values ??(SOA) - Many administrators set their area expiration times too low, which could lead to system downtime if refreshing queries or queries moving the start area has an error. Also, there is no reset of the region's negative-caching TTL when RFC 2308 redefined it, or set the value too high.
7. Wrong type of NS records in your regional data and trust data - some administrators add and subtract authentication servers but forget to request corresponding changes to credentials of the zone via their registration. This can extend the time it takes to resolve domain names in these regions and reduce resiliency.

You finished reading the article "**7 issues to avoid when deploying DNS**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.