DNSreport Results for zimbra.org

Overall Results:

2	**1**	**12**	**5**
FAIL	WARNING	PASS	INFO

PARENT

Status	Test Name	Information
WARN	Parent zone provides NS records	Parent zone does not provide glue for nameservers, which will cause delays in resolving your domain name. The following nameserver addresses were not provided by the parent 'glue' and had to be looked up individually. This is perfectly acceptable behavior per the RFCs. This will usually occur if your DNS servers are not in the same TLD as your domain (for example, a DNS server of "ns1.example.org" for the domain "example.com"). In this case, you can speed up the connections slightly by having NS records that are in the same TLD as your domain. ns2.p28.dynect.net. | No Glue | TTL=86400 ns4.p28.dynect.net. | No Glue | TTL=86400 ns3.p28.dynect.net. | No Glue | TTL=86400 ns1.p28.dynect.net. | No Glue | TTL=86400
PASS	Number of nameservers	At least 2 (RFC2182 section 5 recommends at least 3), but fewer than 8 NS records exist (RFC1912 section 2.8 recommends that you have no more than 7). This meets the RFC minimum requirements, but is lower than the upper limits that some domain registrars have on the number of nameservers. A larger number of nameservers reduce the load on each and, since they should be located in different locations, prevent a single point of failure. The NS Records provided are: ns2.p28.dynect.net. | No Glue | TTL=86400 ns4.p28.dynect.net. | No Glue | TTL=86400 ns3.p28.dynect.net. | No Glue | TTL=86400 ns1.p28.dynect.net. | No Glue | TTL=86400

NS

Status	Test Name	Information
PASS	Unique nameserver IPs	All nameserver addresses are unique. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data:
PASS	All nameservers respond	All nameservers responded. We were able to get a timely response for NS records from your nameservers, which indicates that they are running correctly and your zone (domain) is valid. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data:
PASS	Open DNS servers	Nameservers do not respond to recursive queries. Your DNS servers do not announce that they are open DNS servers (i.e. answering recursively). Although there is a slight chance that they really are open DNS servers, this is very unlikely. Open DNS servers increase the chances of cache poisoning, can degrade performance of your DNS, and can cause your DNS servers to be used in an attack, so it is imperative that externally facing DNS servers do not recursively answer queries.
PASS	All nameservers authoritative	All nameservers answered authoritatively for the zone. This indicates that the zones for this domain are set up correctly on your nameservers and that we should be able to get good responses to further queries.
PASS	NS list matches parent list	NS list matches list from parent zone. This indicates that your parent nameservers are 'aware' of the correct authoritative nameservers for your domain. This ensures less overhead for DNS queries, because an extra DNS resolution step is not required.
PASS	NS address list matches parent zone	NS addresses matches list from parent zone. This indicates that your parent nameservers are 'aware' of the correct authoritative nameservers for your domain. This ensures less overhead for DNS queries, because an extra DNS resolution step is not required.
PASS	Stealth nameservers	No stealth nameservers discovered. There is very little chance that there will be 'confusion' when resolving your domain records from the parent nameservers. There appear to be no 'extra' nameservers listed that the parent might try to refer to and cause DNS resolution delays.
INFO	Stealth nameservers respond	No stealth nameservers to test. This is simply a note to indicate that you do not have any stealth nameservers to test, which is what is normally expected of domains.
PASS	TCP allowed	All nameservers respond to queries via TCP. It is important that your DNS servers respond to both TCP and UDP connections. TCP Port 53 is used for large queries and responses, zone transfers, and is part of the DNSSEC standard.
PASS	Nameserver software version	Responses from nameservers do not appear to be version numbers. While version information is important internally, DNS version information displayed externally can leave your servers vulnerable to version-specific exploits. Your servers appear to hide this information and are likely safer.
PASS	All nameservers have identical records	All of your nameservers are providing the same list of nameservers.
PASS	All nameserver addresses are public	All of your nameserver addresses are public. If there were any private IPs, they would not be reachable, causing DNS delays.

SOA

Status	Test Name	Information
FAIL	SOA record check	No nameservers provided an SOA record for the zone. You should configure your nameservers to have a master slave relationship. The update of the zone information to the slave nameservers should be handled through the SOA record.

MX

Status	Test Name	Information
FAIL	MX records check	No MX records exist within the zone. This is legal, but if you want to receive E-mail on this domain, you should have MX record(s). The program can't continue in a case like this, so we are assuming you don't receive mail on this domain.

WWW

Status	Test Name	Information
INFO	WWW record check	Domain has no WWW hostname record.
INFO	Domain record	The domain literal has no address records.

DNSSEC

Status	Test Name	Information
INFO	DNSSEC records check	No DNSSEC records created for this zone. Many major institutions and government agencies are planning to move to DNSSEC. You may want to consider an implementation plan for the zone specified. If you implemented DNSSEC for your zone we would be able to run further tests.

SPF

Status	Test Name	Information
INFO	SPF record check	This domain does not have an SPF record, nor an SPF formatted TXT record. SPF stands for Sender Policy Framework and is intended as an anti-forgery email solution (See RFC4408). Many spammers have adopted this mechanism and SPF records alone may not be sufficient to stop spam.