DNSreport Results for albinsurance.com

Overall Results:

2	2	27	5
FAIL	WARNING	PASS	INFO

PARENT

Status	Test Name	Information
PASS	Parent zone provides NS records	Parent zone exists and provides NS records. This is good because some domains, usually third or fourth level domains, such as 'example.co.us' do not have a direct parent zone. This is legal but can cause confusion. The NS Records provided are (nameserver | IP Address | TTL): ns11.domaincontrol.com. | 216.69.185.6 ns12.domaincontrol.com. | 173.201.73.6 ns11.domaincontrol.com. | 2607:f208:206::6 ns12.domaincontrol.com. | 2603:5:2290::6
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: ns11.domaincontrol.com. | 216.69.185.6 | TTL=172800 ns12.domaincontrol.com. | 173.201.73.6 | TTL=172800 ns11.domaincontrol.com. | 2607:f208:206::6 | TTL=172800 ns12.domaincontrol.com. | 2603:5:2290::6 | TTL=172800

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: ns11.domaincontrol.com. | No Glue ns12.domaincontrol.com. | No Glue
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: ns11.domaincontrol.com. | No Glue ns12.domaincontrol.com. | No Glue
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
PASS	SOA record check	All nameservers provided a SOA record for the zone. This is good because your nameservers should be configured in a master slave relationship, which allows uniform updates and agreement of resource record data. The SOA records provided are: Primary nameserver: ns11.domaincontrol.com. Hostmaster E-mail address: dns@jomax.net. Serial #: 2018061802 Refresh: 28800 Retry: 7200 Expire: 604800 Minimum: 600
PASS	SOA serial agreement	All nameserver SOAs agree on the serial number. This means that your nameservers are using the same data (unless you have different sets of data with the same serial number, which would be very bad)!
WARN	SOA field check	One or more SOA fields are outside recommended ranges. Values that are out of specifications could cause delays in record updates or unnecessary network traffic. The SOA fields out of range are: expire | 604800 | EXPIRE - RFC1912 suggests a value between 1209600 to 2419200.

MX

Status	Test Name	Information
PASS	MX records check	Two or more different MX records exist within the zone. This is good and ensures consistent and fail-safe mail deliverability. The MX records are: preference = 0 smtp.secureserver.net. [68.178.213.37] preference = 10 mailstore1.secureserver.net. [72.167.238.32]
PASS	Differing mailserver addresses	All hostnames referenced by MX records resolve to different IP addresses. It is important that you have different IP addresses for your MX records, as it ensures that there is not a single point of failure for mail delivery. The hostname IP addresses are: 216.69.185.6 has smtp.secureserver.net. | 68.178.213.37 listed. 216.69.185.6 has mailstore1.secureserver.net. | 72.167.238.32 listed. 173.201.73.6 has smtp.secureserver.net. | 68.178.213.37 listed. 173.201.73.6 has mailstore1.secureserver.net. | 72.167.238.32 listed.
PASS	Reverse DNS entries for MX servers	All addresses referenced by MX records have matching reverse DNS entries. This is good because many mail platforms and spam-prevention schemes require consistency between MX hostnames and IP address PTR records, aka reverse DNS.

MAIL

Status	Test Name	Information
PASS	All IP addresses public	All mailserver IP addresses are public. If there were any private IPs, they would not be reachable.
PASS	Connect to mail server	All connections to Mailservers port 25 are successful. The standard port for SMTP transactions is 25, so your servers should be operating on that port. The Mailserver addresses are: 68.178.213.37 | connected 72.167.238.32 | connected
PASS	SMTP banner	All banner greetings comply with SMTP specified format. 68.178.213.37 | 220 p3plibsmtp02-10.prod.phx3.secureserver.net bizsmtp ESMTP server ready 72.167.238.32 | 220 p3plibsmtp01-15.prod.phx3.secureserver.net bizsmtp ESMTP server ready
WARN	SMTP greeting	Malformed greeting or no A records found matching banner text for following servers, and banner is not an address literal. RFC5321 requires one or the other (should not be a CNAME). If this is not set correctly, some mail platforms will reject or delay mail from you, and can cause hard to diagnose issues with deliverability. Mailserver details: 68.178.213.37 | WARNING: The hostname in the SMTP greeting does not match the reverse DNS (PTR) record for your mail server. This probably won't cause any harm, but may be a technical violation of RFC5321 72.167.238.32 | WARNING: The hostname in the SMTP greeting does not match the reverse DNS (PTR) record for your mail server. This probably won't cause any harm, but may be a technical violation of RFC5321
PASS	Acceptance of NULL sender	Mailserver accepts mail from the null sender address. Mailservers are required to accept mail from a null sender, because this is how delivery status notifications/DSNs are delivered. 68.178.213.37 | 250 2.1.0 <> sender ok 72.167.238.32 | 250 2.1.0 <> sender ok
FAIL	Acceptance of postmaster	Mailserver rejected mail to postmaster. Mailservers are required by RFC822 6.3, RFC1123 5.2.7, and RFC2821 4.5.1 to have a valid postmaster address that is accepting mail. The Mailserver provided is: 68.178.213.37 | unexpected response to [RCPT TO: <postmaster@albinsurance.com>] | 550 5.1.1 <postmaster@albinsurance.com> Recipient not found. <http://x.co/irbounce> 72.167.238.32 | unexpected response to [RCPT TO: <postmaster@albinsurance.com>] | 550 5.1.1 <postmaster@albinsurance.com> Recipient not found. <http://x.co/irbounce>
FAIL	Acceptance of abuse	Mailserver rejected mail to abuse. Mailservers are required by RFC2142 Section 2 to have a valid abuse address that is accepting mail. 68.178.213.37 | unexpected response to [RCPT TO: <abuse@albinsurance.com>] | 550 5.1.1 <abuse@albinsurance.com> Recipient not found. <http://x.co/irbounce> 72.167.238.32 | unexpected response to [RCPT TO: <abuse@albinsurance.com>] | 550 5.1.1 <abuse@albinsurance.com> Recipient not found. <http://x.co/irbounce>

Status	Test Name	Information
INFO	Acceptance of address literals	Mailserver rejected mail to address literals. Mailservers are technically required by RFC1123 section 5.2.17 to accept mail to domain literals (i.e. IP addresses instead of domains). This ensures backwards compatibility and can help with delivery in certain non-optimal situations, like a DNS server being down/unresponsive. 68.178.213.37 | unexpected response to [RCPT TO: <postmaster@[68.178.213.37]>] | 550 5.1.1 <postmaster@[68.178.213.37]> Recipient not found. <http://x.co/irbounce> 72.167.238.32 | unexpected response to [RCPT TO: <postmaster@[72.167.238.32]>] | 550 5.1.1 <postmaster@[72.167.238.32]> Recipient not found. <http://x.co/irbounce>
PASS	Open relay	Mailserver does not appear to be an open relay. This is good. It is important to make sure that external mail servers do not relay mail for domains they are not authoritative for, so that they cannot be abused by third-parties to send unauthorized mail. 68.178.213.37 | 550 5.1.1 <open.relay@example.com> Recipient not found. <http://x.co/irbounce> 72.167.238.32 | 550 5.1.1 <open.relay@example.com> Recipient not found. <http://x.co/irbounce>

WWW

Status	Test Name	Information
INFO	WWW record check	Domain has a WWW hostname provided through one or more CNAME lookups, which will slow down clients attempting to resolve this host. www.albinsurance.com. | consumer.insurancewebsitebuilder.com. | 3600
PASS	Domain record	The domain literal has an address record, the records found are: albinsurance.com. | 69.93.203.211 | 3600
PASS	IP Address(es) valid	All addresses are public. If there were any private IPs, they would not be reachable, causing problems reaching your web site.
PASS	WWW enabled	We connected to WWW, the title data found is: 69.93.203.211 : ALB Insurance Marketing Home Page
PASS	SSL enabled	SSL is enabled. This is good since this will encrypt data that passes from your customer's computer to your website, helping to prevent hackers from using this data. The certificate data is: 69.93.203.211 : certificate issuer [C = US, O = DigiCert Inc, OU = www.digicert.com, CN = RapidSSL RSA CA 2018]; subject [CN = *.insurancewebsitebuilder.com]

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.