DNSreport Results for Vondelphia.com

Overall Results:

1 FAIL

5 WARNING

21 PASS

4 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): `ns2.Vondelphia.com.	167.160.175.245` `ns1.Vondelphia.com.	167.160.175.245`
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.Vondelphia.com.	167.160.175.245	TTL=172800` `ns1.Vondelphia.com.	167.160.175.245	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: `ns1.von.host.	167.160.175.245` `ns2.von.host.	167.160.175.245`
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: `ns1.von.host.	167.160.175.245` `ns2.von.host.	167.160.175.245`
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.
WARN	NS list matches parent list	NS list does not match list from parent zone. This should be addressed because queries for this domain may require an extra lookup (and more overhead) because there is no direct relationship between the NS records at the parent and the NS records at the authoritative servers. This can cause delays. The mismatched NS list is: `nameserver ns2.von.host.	167.160.175.245 is missing ns2.Vondelphia.com.	167.160.175.245` `nameserver ns2.von.host.	167.160.175.245 is missing ns1.Vondelphia.com.	167.160.175.245`
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.
WARN	Stealth nameservers	One or more stealth nameservers discovered. This means that one or more nameservers are not listed at both the parent and authoritative nameservers. This can be confusing and can cause delays or other hard to diagnose inconsistencies. The stealth nameservers discovered are: `ns2.von.host. has nameserver ns1.von.host.	167.160.175.245 listed where other nameservers do not.` `ns2.von.host. has nameserver ns2.von.host.	167.160.175.245 listed where other nameservers do not.`
PASS	Stealth nameservers respond	All stealth nameservers respond. While having stealth nameservers can be problematic, the ones that exist are responding to queries, which can limit the negative impact of having them in the first place.
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.
WARN	Nameserver software version	One or more nameservers responded to version queries. This can be considered a breach of security. If a malicious person or program had access to a version-specific exploit for your DNS server, displaying the version info openly will make their attack much easier. This should be removed or obscured. The nameservers that responded to version queries are: `167.160.175.245 responded with "9.11.4-P2-RedHat-9.11.4-9.P2.el7"`
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: ns1.von.host.`
		`Hostmaster E-mail address: matt@maggew.com.`
		`Serial #: 2020041400`
		`Refresh: 3600`
		`Retry: 7200`
		`Expire: 1209600`
		`Minimum: 86400`

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: `mname	ns1.von.host.	MNAME - we check that this name matches one of the nameservers that we have found.` `retry	7200	RETRY - needs to be less than or equal to half the REFRESH.`

MX

Status	Test Name	Information
WARN	MX records check	Only one MX record exists within the zone. This is ok, but it is a better practice to have at least two mail servers operating on a domain, to ensure more reliable mail deliverability. The MX record provided is: `preference = 0 vondelphia.com. [167.160.175.245]`
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: `167.160.175.245 has vondelphia.com.	167.160.175.245 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.
FAIL	Connect to mail server	All connections to Mailservers port 25 have failed. The standard port for SMTP transactions is 25, so your servers should be operating on that port. It is recommended that it be fixed in order for your mail service to operate properly. The Mail Servers that failed are: `167.160.175.245	failed message send with: messaging failure: Time out occurred or Remote server closed connection prematurely`

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.Vondelphia.com.	vondelphia.com.	14400` `vondelphia.com.	167.160.175.245	14400`
PASS	Domain record	The domain literal has an address record, the records found are: `Vondelphia.com.	167.160.175.245	14400`
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: `167.160.175.245 : 301 Moved`
INFO	SSL enabled	SSL is not enabled. This is ok, but if your website offers online shopping or other private services, you should acquire an SSL cert and enable SSL. SSL will encrypt the data communication between your site and customers, helping to prevent private data from being intercepted and read.

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 has an SPF record, or an SPF formatted TXT record. SPF usage may have a negligible impact on spam prevention and if implemented incorrectly cause serious mail delivery problems for remote users. This software does not check the content of your SPF record to test if it is well designed only that it exists. Your SPF record(s) for each nameserver is/are: `"v=spf1 a mx ip4:167.160.175.245 ip4:45.63.16.106 ~all"`
PASS	SPF formatted TXT record exists	An SPF formatted TXT record was found. This configuration is in wide use as a verification mechanism. Note: this test does not verify the design of this record only that it exists (listing includes one for each nameserver). `"v=spf1 a mx ip4:167.160.175.245 ip4:45.63.16.106 ~all"`
PASS	SPF value covers incoming mailservers	The SPF value allows mail delivery from all mailservers in the domain. The SPF results are: `domain of Vondelphia.com designates 167.160.175.245 as permitted sender`

Status	Test Name	Information
	SPF record check	This domain has an SPF record, or an SPF formatted TXT record. SPF usage may have a negligible impact on spam prevention and if implemented incorrectly cause serious mail delivery problems for remote users. This software does not check the content of your SPF record to test if it is well designed only that it exists. Your SPF record(s) for each nameserver is/are: `"v=spf1 a mx ip4:167.160.175.245 ip4:45.63.16.106 ~all"`
PASS	SPF formatted TXT record exists	An SPF formatted TXT record was found. This configuration is in wide use as a verification mechanism. Note: this test does not verify the design of this record only that it exists (listing includes one for each nameserver). `"v=spf1 a mx ip4:167.160.175.245 ip4:45.63.16.106 ~all"`
PASS	SPF value covers incoming mailservers	The SPF value allows mail delivery from all mailservers in the domain. The SPF results are: `domain of Vondelphia.com designates 167.160.175.245 as permitted sender`