Tools

DNSreport for ospito.nl

Generated by www.DNSreport.com at 21:35:57 GMT on 24 Aug 2008.

Email link to results

Category	Status	Test Name	Information
Parent	PASS	Missing Direct Parent check	OK. Your direct parent zone exists, which is good. Some domains (usually third or fourth level domains, such as example.co.us) do not have a direct parent zone ('co.us' in this example), which is legal but can cause confusion.

	INFO	NS records at parent servers	Your NS records at the parent servers are:
			
			`ns2.ospito.net. [83.96.152.10 (NO GLUE)] [NL]`
			`ns1.ospito.nl. [77.243.226.26] [TTL=7200] [NL]`
			`ns3.ospito.eu. [82.201.99.246 (NO GLUE)] [NL]`
			[These were obtained from ns-ext.isc.org]

	PASS	Parent nameservers have your nameservers listed	OK. When someone uses DNS to look up your domain, the first step (if it doesn't already know about your domain) is to go to the parent servers. If you aren't listed there, you can't be found. But you are listed there.
	WARN	Glue at parent nameservers	WARNING. The parent servers (I checked with ns-ext.isc.org.) are not providing glue for all your nameservers. This means that they are supplying the NS records (host.example.com), but not supplying the A records (192.0.2.53), which can cause slightly slower connections, and may cause incompatibilities with some non-RFC-compliant programs. 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.

	PASS	DNS servers have A records	OK. All your DNS servers either have A records at the zone parent servers, or do not need them (if the DNS servers are on other TLDs). A records are required for your hostnames to ensure that other DNS servers can reach your DNS servers. Note that there will be problems if your DNS servers do not have these same A records.

NS	INFO	NS records at your nameservers	Your NS records at your nameservers are:
			
			`ns1.ospito.nl. [77.243.226.26] [TTL=300]`
			`ns3.ospito.eu. [82.201.99.246] [TTL=300]`
			`ns2.ospito.net. [83.96.152.10] [TTL=300]`

	PASS	Open DNS servers	OK. Your DNS servers do not announce that they are open DNS servers. Although there is a slight chance that they really are open DNS servers, this is very unlikely. Open DNS servers increase the chances that of cache poisoning, can degrade performance of your DNS, and can cause your DNS servers to be used in an attack (so it is good that your DNS servers do not appear to be open DNS servers).
	PASS	Mismatched glue	OK. The DNS report did not detect any discrepancies between the glue provided by the parent servers and that provided by your authoritative DNS servers.
	PASS	No NS A records at nameservers	OK. Your nameservers do include corresponding A records when asked for your NS records. This ensures that your DNS servers know the A records corresponding to all your NS records.
	PASS	All nameservers report identical NS records	OK. The NS records at all your nameservers are identical.
	PASS	All nameservers respond	OK. All of your nameservers listed at the parent nameservers responded.
	PASS	Nameserver name validity	OK. All of the NS records that your nameservers report seem valid (no IPs or partial domain names).
	PASS	Number of nameservers	OK. You have 3 nameservers. You must have at least 2 nameservers (RFC2182 section 5 recommends at least 3 nameservers), and preferably no more than 7.
	PASS	Lame nameservers	OK. All the nameservers listed at the parent servers answer authoritatively for your domain.
	PASS	Missing (stealth) nameservers	OK. All 3 of your nameservers (as reported by your nameservers) are also listed at the parent servers.
	PASS	Missing nameservers 2	OK. All of the nameservers listed at the parent nameservers are also listed as NS records at your nameservers.
	PASS	No CNAMEs for domain	OK. There are no CNAMEs for ospito.nl. RFC1912 2.4 and RFC2181 10.3 state that there should be no CNAMEs if an NS (or any other) record is present.
	PASS	No NSs with CNAMEs	OK. There are no CNAMEs for your NS records. RFC1912 2.4 and RFC2181 10.3 state that there should be no CNAMEs if an NS (or any other) record is present.
	WARN	Nameservers on separate class C's	WARNING: We cannot test to see if your nameservers are all on the same Class C (technically, /24) range, because the root servers are not sending glue. We plan to add such a test later, but today you will have to manually check to make sure that they are on separate Class C ranges. Your nameservers should be at geographically dispersed locations. You should not have all of your nameservers at the same location. RFC2182 3.1 goes into more detail about secondary nameserver location.
	PASS	All NS IPs public	OK. All of your NS records appear to use public IPs. If there were any private IPs, they would not be reachable, causing DNS delays.
			OK. All your DNS servers allow TCP connections. Although rarely used, TCP connections are occasionally used instead of

	PASS	TCP Allowed	UDP connections. When firewalls block the TCP DNS connections, it can cause hard-to-diagnose problems.
	INFO	Nameservers versions	Your nameservers have the following versions: 83.96.152.10: "Ospito Internet Domain Name System: ns2.ospito.net" 77.243.226.26: "Ospito Internet Domain Name System: ns1.ospito.nl" 82.201.99.246: "Ospito Internet Domain Name System: ns3.ospito.eu"
	PASS	Stealth NS record leakage	Your DNS servers do not leak any stealth NS records (if any) in non-NS requests.

SOA	INFO	SOA record	Your SOA record [TTL=300] is:
			
			`Primary nameserver: ns1.ospito.nl.`
			`Hostmaster E-mail address: hostmaster.ospito.nl.`
			`Serial #: 2008081700`
			`Refresh: 14400`
			`Retry: 3600`
			`Expire: 1209600`
			`Default TTL: 86400`

	PASS	NS agreement on SOA Serial #	OK. All your nameservers agree that your SOA serial number is 2008081700. That means that all your nameservers are using the same data (unless you have different sets of data with the same serial number, which would be very bad)! Note that the DNSreport only checks the NS records listed at the parent servers (not any stealth servers).
	PASS	SOA MNAME Check	OK. Your SOA (Start of Authority) record states that your **master** (primary) name server is: **ns1.ospito.nl.**. That server is listed at the parent servers, which is correct.
	PASS	SOA RNAME Check	OK. Your SOA (Start of Authority) record states that your DNS contact E-mail address is: **hostmaster@ospito.nl.** (techie note: we have changed the initial '.' to an '@' for display purposes).
	PASS	SOA Serial Number	OK. Your SOA serial number is: **2008081700**. This appears to be in the recommended format of YYYYMMDDnn, where 'nn' is the revision. So this indicates that your DNS was last updated on 17 Aug 2008 (and was revision #0). This number **must** be incremented every time you make a DNS change.
	PASS	SOA REFRESH value	OK. Your SOA REFRESH interval is : **14400 seconds**. This seems normal (about 3600-7200 seconds is good if not using DNS NOTIFY; RFC1912 2.2 recommends a value between 1200 to 43200 seconds (20 minutes to 12 hours)). This value determines how often secondary/slave nameservers check with the master for updates.
	PASS	SOA RETRY value	OK. Your SOA RETRY interval is : **3600 seconds**. This seems normal (about 120-7200 seconds is good). The retry value is the amount of time your secondary/slave nameservers will wait to contact the master nameserver again if the last attempt failed.
	PASS	SOA EXPIRE value	OK. Your SOA EXPIRE time: **1209600 seconds**. This seems normal (about 1209600 to 2419200 seconds (2-4 weeks) is good). RFC1912 suggests 2-4 weeks. This is how long a secondary/slave nameserver will wait before considering its DNS data stale if it can't reach the primary nameserver.
	PASS	SOA MINIMUM TTL value	OK. Your SOA MINIMUM TTL is: **86400 seconds**. This seems normal (about 3,600 to 86400 seconds or 1-24 hours is good). RFC2308 suggests a value of 1-3 hours. This value used to determine the default (technically, minimum) TTL (time-to-live) for DNS entries, but now is used for negative caching.
			Your 4 MX records are:

MX	**INFO**	MX Record	10 mail.ospito.nl. [TTL=300] IP=77.243.226.77 [TTL=300] [NL] 20 fallback1.ospito.nl. [TTL=300] IP=77.243.226.27 [TTL=300] [NL] 30 fallback2.ospito.nl. [TTL=300] IP=83.96.152.11 [TTL=300] [NL] 40 fallback3.ospito.nl. [TTL=300] IP=82.201.99.247 [TTL=300] [NL]
	PASS	Low port test	OK. Our local DNS server that uses a low port number can get your MX record. Some DNS servers are behind firewalls that block low port numbers. This does not guarantee that your DNS server does not block low ports (this specific lookup must be cached), but is a good indication that it does not.
	PASS	Invalid characters	OK. All of your MX records appear to use valid hostnames, without any invalid characters.
	PASS	All MX IPs public	OK. All of your MX records appear to use public IPs. If there were any private IPs, they would not be reachable, causing slight mail delays, extra resource usage, and possibly bounced mail.
	PASS	MX records are not CNAMEs	OK. Looking up your MX record did not just return a CNAME. If an MX record query returns a CNAME, extra processing is required, and some mail servers may not be able to handle it.
	PASS	MX A lookups have no CNAMEs	OK. There appear to be no CNAMEs returned for A records lookups from your MX records (CNAMEs are prohibited in MX records, according to RFC974, RFC1034 3.6.2, RFC1912 2.4, and RFC2181 10.3).
	PASS	MX is host name, not IP	OK. All of your MX records are host names (as opposed to IP addresses, which are not allowed in MX records).
	PASS	Multiple MX records	OK. You have multiple MX records. This means that if one is down or unreachable, the other(s) will be able to accept mail for you.
	PASS	Differing MX-A records	OK. I did not detect differing IPs for your MX records (this would happen if your DNS servers return different IPs than the DNS servers that are authoritative for the hostname in your MX records).
	PASS	Duplicate MX records	OK. You do not have any duplicate MX records (pointing to the same IP). Although technically valid, duplicate MX records can cause a lot of confusion, and waste resources.
	PASS	Reverse DNS entries for MX records	OK. The IPs of all of your mail server(s) have reverse DNS (PTR) entries. RFC1912 2.1 says you should have a reverse DNS for all your mail servers. It is strongly urged that you have them, as many mailservers will not accept mail from mailservers with no reverse DNS entry. Note that this information is *cached*, so if you changed it recently, it will not be reflected here (see the www.DNSstuff.com Reverse DNS Tool for the current data). The reverse DNS entries are: 77.226.243.77.in-addr.arpa **rome.ospito.nl.** [TTL=299] 27.226.243.77.in-addr.arpa **fallback1.ospito.nl.** [TTL=299] 11.152.96.83.in-addr.arpa **fallback2.ospito.net.** [TTL=299] 247.99.201.82.in-addr.arpa **fallback3.ospito.eu.** [TTL=86400]
	PASS	Connect to mail servers	OK: I was able to connect to all of your mailservers.
	PASS	Mail server host name in greeting	OK: All of your mailservers have their host name in the greeting: fallback2.ospito.nl: 220 **fallback2.ospito.net** ESMTP Postfix fallback1.ospito.nl: 220 **fallback1.ospito.nl** ESMTP Postfix fallback3.ospito.nl: 220 **fallback3.ospito.eu** ESMTP Postfix mail.ospito.nl: 220 **rome.ospito.nl** ESMTP Exim 4.69 Sun, 24 Aug 2008 23:35:59 +0200
	PASS	Acceptance of NULL <> sender	OK: All of your mailservers accept mail from "<>". You are required (RFC1123 5.2.9) to receive this type of mail (which includes reject/bounce messages and return receipts).

Mail	PASS	Acceptance of postmaster address	OK: All of your mailservers accept mail to postmaster@ospito.nl (as required by RFC822 6.3, RFC1123 5.2.7, and RFC2821 4.5.1).
	PASS	Acceptance of abuse address	OK: All of your mailservers accept mail to abuse@ospito.nl.
	INFO	Acceptance of domain literals	WARNING: One or more of your mailservers does not accept mail in the domain literal format (user@[0.0.0.0]). Mailservers are technically required RFC1123 5.2.17 to accept mail to domain literals for any of its IP addresses. Not accepting domain literals can make it more difficult to test your mailserver, and can prevent you from receiving E-mail from people reporting problems with your mailserver. However, it is unlikely that any problems will occur if the domain literals are not accepted (mailservers at many common large domains have this problem). `mail.ospito.nl's postmaster@[77.243.226.77] response:  >>> RCPT TO:<postmaster@[77.243.226.77]>  <<< 501 <postmaster@[77.243.226.77]>: domain literals not allowed `
	PASS	Open relay test	OK: All of your mailservers appear to be closed to relaying. This is *not* a thorough check, you can get a thorough one here. `mail.ospito.nl OK: 550 authentication required fallback2.ospito.nl OK: 554 5.7.1 <Not.abuse.see.www.DNSreport.com.from.IP.77.61.239.25@DNSreport.com>: Relay access denied fallback1.ospito.nl OK: 554 5.7.1 <Not.abuse.see.www.DNSreport.com.from.IP.77.61.239.25@DNSreport.com>: Relay access denied fallback3.ospito.nl OK: 554 5.7.1 <Not.abuse.see.www.DNSreport.com.from.IP.77.61.239.25@DNSreport.com>: Relay access denied `
	PASS	SPF record	You have an SPF record. This is very good, as it will help prevent spammers from abusing your domain. Your SPF record (I don't check to see if it is well designed!) is: `"v=spf1 ip4:77.243.226.77 ~all" [TTL=300]`
WWW	INFO	WWW Record	Your www.ospito.nl A record is: `www.ospito.nl. A 77.243.226.77 [TTL=300] [NL]`
	PASS	All WWW IPs public	OK. All of your WWW IPs appear to be public IPs. If there were any private IPs, they would not be reachable, causing problems reaching your web site.
	PASS	CNAME Lookup	OK. Some domains have a CNAME record for their WWW server that requires an extra DNS lookup, which slightly delays the initial access to the website and use extra bandwidth. There are no CNAMEs for www.ospito.nl, which is good.
	INFO	Domain A Lookup	Your ospito.nl A record is: `ospito.nl. A 77.243.226.77 [TTL=300]`

Legend:

- UPDATE NOTICE November 2007:
  We have made the decision to remove the Single Point of Failure test included in DNSreport. This test was developed and enhanced over the past five years along with our other tools. The initial design of the Single Point of Failure test depended on the typical connectivity profiles prevalent at the time. As connectivity has

become more robust the methodology employed makes less sense and creates more false positives. Our development team is working on an enhanced Single Point of Failure test for a future release.

- Rows with a FAIL indicate a problem that in most cases really should be fixed.
- Rows with a WARN indicate a possible minor problem, which often is not worth pursuing.
- Note that all information is accessed in real-time (except where noted), so this is the freshest information about your domain.
- Note that *automated usage* is not tolerated without the purchase of an Automated Usage plan; please only view the DNS report directly with your web browser.


Email link to results