



<b>Organization Name:</b>	Example
<b>Contact Name:</b>	Your Contact Here
<b>Contact E-Mail:</b>	Contact@Here
<b>Report Date:</b>	Fri Aug 17 16:46:06 2007
<b>Dns Advisor Version:</b>	v1.0r0-0

This report analyzes the DNS test executed on Fri Aug 17 16:46:06 2007 by Your Contact Here <Contact@Here>. Provided is overall summary and detailed information on the results of this test run. Analysis of the findings can help you determine if any steps are needed to ensure that your network complies with industry best practices. For additional information please contact your authorized Infoblox representative. Send e-mail to [dnsadvisorpro@infoblox.com](mailto:dnsadvisorpro@infoblox.com). Infoblox on the web: [www.infoblox.com](http://www.infoblox.com).

## Summary

### Zone summary

Found 1 zone(s): [example.org](http://example.org).

	Number of tests
<b>Severe problem</b>	<b>1</b>
<b>Serious problem</b>	<b>1</b>
<b>Potential problem</b>	<b>4</b>
<b>Configured correctly</b>	<b>56</b>
<b>Total cases completed</b>	<b>62</b>

### Name server summary

Found 2 name server(s): [a.iana-servers.net](http://a.iana-servers.net), [b.iana-servers.net](http://b.iana-servers.net).

	Number of tests
<b>Potential problem</b>	<b>3</b>
<b>Configured correctly</b>	<b>9</b>
<b>Total cases completed</b>	<b>12</b>

## Detailed Test Results

## Zones

Zone	Severe problem	Serious problem	Potential problem	Configured correctly	Total cases completed
<a href="#">example.org</a>	1	1	4	56	62

### Zone: example.org

<b>T001A</b>	Lookup NS RRs at parent	Found: b.iana-servers.net., a.iana-servers.net.	green
--------------	-------------------------	---	-------

#### Description:

This test checks that delegation is in place from the tested zone's parent to the tested zone.

#### Implication:

If this delegation isn't in place, other name servers won't be able to resolve domain names in the tested zone or its subzones. That means you'll effectively be unreachable: email won't be delivered and users won't be able to reach your web site.

#### Mitigation:

If you find that delegation to the tested zone is missing, make sure you're testing the correct set of parent name servers. By default, the tool works its way down from the Internet's root name servers to find the tested zone's name servers. In split namespaces, this probably isn't the right thing to do. If you have a split namespace, you can use the "Internal root server addresses" section of the "Exceptions" tab to list your internal root name servers' addresses (if you have internal root name servers), or the addresses of your parent zone's name servers, or if none of those apply, just the addresses of your zone's authoritative name servers. If the tool tested the correct set of parent name servers, add the delegation to the parent zone.

<b>T001B</b>	Check >1 NS RR	2 NS records found: b.iana-servers.net., a.iana-servers.net.	green
--------------	----------------	--	-------

#### Description:

This test checks that the delegation to the tested zone includes at least two NS records. Two authoritative name servers is the minimum to provide the necessary redundancy for your zone.

#### Implication:

A single NS record isn't enough to ensure that domain names in your zone will be resolvable: The failure of a single name server will render your zone unreachable.

#### Mitigation:

If you really only have one authoritative name server for your zone, add another. This could be a new secondary name server you set up yourself or an existing name server that you configure to also be secondary for this zone. Then update the delegation to your zone to include this new authoritative name server. If you actually have more than one

authoritative name server, make sure your zone's delegation information in the parent zone is updated to include all of them. It does you no good to run more than one external authoritative name server but only delegate to one.

<b>T001C</b>	<b>Check NS RRs are valid names</b>	<b>a.iana-servers.net. is a valid name</b>	<b>green</b>
--------------	-------------------------------------	--	--------------

**Description:**

This test checks that the domain names of the name servers authoritative for the tested zone are legal. Legal domain names contain alphanumeric characters (A to Z upper- and lowercase, and 0 to 9) and dash.

**Implication:**

Using illegal domain names for your zone's name servers can make it difficult or even impossible for other name servers to resolve domain names in your zone.

**Mitigation:**

Change the domain names of the name servers in your zone's delegation by contacting the administrator of your zone's parent zone, and change the domain names in your zone's NS records, too (i.e., the "intrazone" NS records).

<b>T001C</b>	<b>Check NS RRs are valid names</b>	<b>b.iana-servers.net. is a valid name</b>	<b>green</b>
--------------	-------------------------------------	--	--------------

**Description:**

This test checks that the domain names of the name servers authoritative for the tested zone are legal. Legal domain names contain alphanumeric characters (A to Z upper- and lowercase, and 0 to 9) and dash.

**Implication:**

Using illegal domain names for your zone's name servers can make it difficult or even impossible for other name servers to resolve domain names in your zone.

**Mitigation:**

Change the domain names of the name servers in your zone's delegation by contacting the administrator of your zone's parent zone, and change the domain names in your zone's NS records, too (i.e., the "intrazone" NS records).

<b>T002A</b>	<b>Lookup NS RRs at auth. name servers</b>	<b>a.iana-servers.net. answered NS query with: b.iana-servers.net., a.iana-servers.net.</b>	<b>green</b>
--------------	--	---	--------------

**Description:**

This test checks that the name servers listed in the tested zone's delegation respond with the list of authoritative name servers for the zone. If a name server listed in the delegation for the tested zone doesn't respond with the list of authoritative name servers for the zone, it's probably either down or "lame." ("Lame" means that the zone is delegated to the name server, but the name server isn't authoritative for the zone. That's a no-no.)

**Implication:**

If your zone has one or more down or lame name servers, this will increase the time it takes for remote name servers to resolve your zone's domain names.

#### Mitigation:

If it's down, of course, you should figure out why. Did it crash? Was it moved to another IP address? Was it decommissioned? If it's "lame"--running a name server that's not authoritative for the zone--should the name server be reconfigured as authoritative for the zone? Or was it inadvertently listed in the delegation and should be removed?

<b>T002A</b>	<b>Lookup NS RRs at auth. name servers</b>	<b>b.iana-servers.net. answered NS query with: b.iana-servers.net., a.iana-servers.net.</b>	<b>green</b>
--------------	--	---	--------------

#### Description:

This test checks that the name servers listed in the tested zone's delegation respond with the list of authoritative name servers for the zone. If a name server listed in the delegation for the tested zone doesn't respond with the list of authoritative name servers for the zone, it's probably either down or "lame." ("Lame" means that the zone is delegated to the name server, but the name server isn't authoritative for the zone. That's a no-no.)

#### Implication:

If your zone has one or more down or lame name servers, this will increase the time it takes for remote name servers to resolve your zone's domain names.

#### Mitigation:

If it's down, of course, you should figure out why. Did it crash? Was it moved to another IP address? Was it decommissioned? If it's "lame"--running a name server that's not authoritative for the zone--should the name server be reconfigured as authoritative for the zone? Or was it inadvertently listed in the delegation and should be removed?

<b>T002B</b>	<b>Check &gt;1 NS RR</b>	<b>2 NS records found at a.iana-servers.net.</b>	<b>green</b>
--------------	--------------------------	--	--------------

#### Description:

This test checks that the delegation to the tested zone includes at least two NS records. Two authoritative name servers is the minimum to provide the necessary redundancy for your zone.

#### Implication:

A single NS record isn't enough to ensure that domain names in your zone will be resolvable: The failure of a single name server will render your zone unreachable.

#### Mitigation:

If you really only have one authoritative name server for your zone, add another. This could be a new secondary name server you set up yourself or an existing name server that you configure to also be secondary for this zone. Then update the delegation to your zone to include this new authoritative name server. If you actually have more than one authoritative name server, make sure your zone's delegation information in the parent zone is updated to include all of them. It does you no good to run more than one external authoritative name server but only delegate to one.

<b>T002B</b>	<b>Check &gt;1 NS RR</b>	<b>2 NS records found at b.iana-servers.net.</b>	<b>green</b>
--------------	--------------------------	--	--------------

**Description:**

This test checks that the delegation to the tested zone includes at least two NS records. Two authoritative name servers is the minimum to provide the necessary redundancy for your zone.

**Implication:**

A single NS record isn't enough to ensure that domain names in your zone will be resolvable: The failure of a single name server will render your zone unreachable.

**Mitigation:**

If you really only have one authoritative name server for your zone, add another. This could be a new secondary name server you set up yourself or an existing name server that you configure to also be secondary for this zone. Then update the delegation to your zone to include this new authoritative name server. If you actually have more than one authoritative name server, make sure your zone's delegation information in the parent zone is updated to include all of them. It does you no good to run more than one external authoritative name server but only delegate to one.

<b>T002C</b>	<b>Check NS RRs are valid names</b>	<b>a.iana-servers.net. is a valid name</b>	<b>green</b>
--------------	-------------------------------------	--	--------------

**Description:**

This test checks that the domain names of the name servers authoritative for the tested zone are legal. Legal domain names contain alphanumeric characters (A to Z upper- and lowercase, and 0 to 9) and dash.

**Implication:**

Using illegal domain names for your zone's name servers can make it difficult or even impossible for other name servers to resolve domain names in your zone.

**Mitigation:**

Change the domain names of the name servers in your zone's delegation by contacting the administrator of your zone's parent zone, and change the domain names in your zone's NS records, too (i.e., the "intrazone" NS records).

<b>T002C</b>	<b>Check NS RRs are valid names</b>	<b>b.iana-servers.net. is a valid name</b>	<b>green</b>
--------------	-------------------------------------	--	--------------

**Description:**

This test checks that the domain names of the name servers authoritative for the tested zone are legal. Legal domain names contain alphanumeric characters (A to Z upper- and lowercase, and 0 to 9) and dash.

**Implication:**

Using illegal domain names for your zone's name servers can make it difficult or even impossible for other name servers to resolve domain names in your zone.

**Mitigation:**

Change the domain names of the name servers in your zone's delegation by contacting the administrator of your zone's parent zone, and change the domain names in your zone's NS records, too (i.e., the "intrazone" NS records).

**T002D****Compare auth and parent NS RR sets****a.iana-servers.net. NS RRs match the parent set****green****Description:**

This test checks that the NS records that delegate the tested zone from its parent and the NS records in the tested zone match. The NS records that delegate your zone from its parent and the NS records in your zone should match.

**Implication:**

Mismatched NS records will usually cause problems resolving domain names in your zone, including longer resolution times and reduced redundancy.

**Mitigation:**

Adjust the NS records in your zone and those in your zone's parent so that they match.

**T002D****Compare auth and parent NS RR sets****b.iana-servers.net. NS RRs match the parent set****green****Description:**

This test checks that the NS records that delegate the tested zone from its parent and the NS records in the tested zone match. The NS records that delegate your zone from its parent and the NS records in your zone should match.

**Implication:**

Mismatched NS records will usually cause problems resolving domain names in your zone, including longer resolution times and reduced redundancy.

**Mitigation:**

Adjust the NS records in your zone and those in your zone's parent so that they match.

**T003A****Lookup A RRs for NS names****a.iana-servers.net. resolves to 192.0.34.43****green****Description:**

This test checks that each name server listed in an NS record has at least one A record (and hence at least one IP address) associated with it. If a name server is listed in an NS record and has no A record associated with it, there's no way for another name server to query it.

**Implication:**

Listing a name server with no A record is effectively the same as not running that name server at all, and will lead to longer resolution times and reduced redundancy.

**Mitigation:**

Check whether the domain name of the name server is misspelled in the NS record. If not, check whether the A record for the name server is missing.

<b>T003A</b>	<b>Lookup A RRs for NS names</b>	<b>b.iana-servers.net. resolves to 193.0.0.236</b>	<b>green</b>
--------------	----------------------------------	--	--------------

**Description:**

This test checks that each name server listed in an NS record has at least one A record (and hence at least one IP address) associated with it. If a name server is listed in an NS record and has no A record associated with it, there's no way for another name server to query it.

**Implication:**

Listing a name server with no A record is effectively the same as not running that name server at all, and will lead to longer resolution times and reduced redundancy.

**Mitigation:**

Check whether the domain name of the name server is misspelled in the NS record. If not, check whether the A record for the name server is missing.

<b>T003B</b>	<b>Check for matching glue records</b>	<b>Parent and authoritative glue records match at a.iana-servers.net.</b>	<b>green</b>
--------------	--	---	--------------

**Description:**

This test checks that the A records for each name server match in the delegation for the tested zone and in the tested zone itself.

**Implication:**

Mismatched A records will usually cause problems resolving domain names in your zone, including longer resolution times and reduced redundancy.

**Mitigation:**

Adjust the A records in your zone and those in your zone's parent so that they match.

<b>T003B</b>	<b>Check for matching glue records</b>	<b>Parent and authoritative glue records match at b.iana-servers.net.</b>	<b>green</b>
--------------	--	---	--------------

**Description:**

This test checks that the A records for each name server match in the delegation for the tested zone and in the tested zone itself.

**Implication:**

Mismatched A records will usually cause problems resolving domain names in your zone, including longer resolution times and reduced redundancy.

### Mitigation:

Adjust the A records in your zone and those in your zone's parent so that they match.

<b>T003C</b>	<b>Check NS addresses on &gt;1 network</b>	<b>193.0.0.0, 192.0.34.0</b>	<b>green</b>
--------------	--	------------------------------	--------------

### Description:

This test checks that the tested zone's authoritative name servers are on more than one network. (It uses a simpleminded check to determine whether two name servers are on the same network, comparing the first three octets of their IP addresses. If you know that your name servers are on different networks, despite the first three octets of their IP addresses being the same, you can ignore this error.)

### Implication:

If all of your zone's authoritative name servers are on the same network, you have a single point of failure--perhaps several--in your zone's DNS infrastructure. The failure of a single leased line, router, hub, or switch could render the domain names in your zone unresolvable.

### Mitigation:

Add diversity to your zone's DNS infrastructure by adding a secondary name server on another network. This could be a new secondary you set up yourself or an existing name server that you configure to also be secondary for this zone.

<b>T003D</b>	<b>Check for RFC1918 addresses</b>	<b>NS A record 192.0.34.43 is not RFC1918</b>	<b>green</b>
--------------	------------------------------------	---	--------------

### Description:

This test checks whether any of the tested zone's authoritative name servers are on RFC 1918 (private internal) networks. There are no routes on the Internet to RFC 1918 networks.

### Implication:

If your zone is entirely internal, you can ignore the results of this test. However, for zones that are resolved from the Internet, listing name servers on RFC 1918 networks is about as useful as not listing them at all (in fact, it's actually worse, since name servers on the Internet will waste time trying to query those name servers).

### Mitigation:

Remove any name servers on RFC 1918 networks from your zone's delegation and authoritative data, and replace them with name servers on networks reachable from the Internet.

<b>T003D</b>	<b>Check for RFC1918 addresses</b>	<b>NS A record 193.0.0.236 is not RFC1918</b>	<b>green</b>
--------------	------------------------------------	---	--------------

### Description:

This test checks whether any of the tested zone's authoritative name servers are on RFC 1918 (private internal)

networks. There are no routes on the Internet to RFC 1918 networks.

### Implication:

If your zone is entirely internal, you can ignore the results of this test. However, for zones that are resolved from the Internet, listing name servers on RFC 1918 networks is about as useful as not listing them at all (in fact, it's actually worse, since name servers on the Internet will waste time trying to query those name servers).

### Mitigation:

Remove any name servers on RFC 1918 networks from your zone's delegation and authoritative data, and replace them with name servers on networks reachable from the Internet.

<b>T003E</b>	<b>Check for CNAMEs</b>	<b>a.iana-servers.net. does not own a CNAME</b>	<b>green</b>
--------------	-------------------------	---	--------------

### Description:

This test checks whether any of the tested zone's NS records lists the alias of a name server rather than its official name.

### Implication:

Most name servers on the Internet won't follow an alias to learn the address of a name server, so using an alias in an NS record is about as useful as not listing it at all.

### Mitigation:

Replace any aliases in NS records with the official (or "canonical") domain names of the name servers.

<b>T003E</b>	<b>Check for CNAMEs</b>	<b>b.iana-servers.net. does not own a CNAME</b>	<b>green</b>
--------------	-------------------------	---	--------------

### Description:

This test checks whether any of the tested zone's NS records lists the alias of a name server rather than its official name.

### Implication:

Most name servers on the Internet won't follow an alias to learn the address of a name server, so using an alias in an NS record is about as useful as not listing it at all.

### Mitigation:

Replace any aliases in NS records with the official (or "canonical") domain names of the name servers.

<b>T003F</b>	<b>Check for duplicate NS addr</b>	<b>No duplicated NS addr</b>	<b>green</b>
--------------	------------------------------------	------------------------------	--------------

### Description:

This test looks up the addresses of the authoritative name servers for the zone and checks for duplicates.

**Implication:**

Duplicate address records don't add any redundancy, and may in fact increase resolution time.

**Mitigation:**

Remove NS records that point to duplicate addresses.

<b>T004A</b>	<b>Reverse map all NS A RRs</b>	<b>192.0.34.43 has a PTR record</b>	<b>green</b>
--------------	---------------------------------	-------------------------------------	--------------

**Description:**

This test checks whether the addresses of the tested zone's name servers map back to domain names.

**Implication:**

This is really more of an aesthetic issue than anything else. Query tools like nslookup and dig work better if your name server's address maps back to a domain name.

**Mitigation:**

If your name server's address doesn't map back to a domain name and you control the reverse-mapping zone the address is a part of, just add a PTR record for its address to the reverse-mapping zone. If someone else controls the reverse-mapping zone, ask them to add a PTR record for your name server.

<b>T004A</b>	<b>Reverse map all NS A RRs</b>	<b>193.0.0.236 has a PTR record</b>	<b>green</b>
--------------	---------------------------------	-------------------------------------	--------------

**Description:**

This test checks whether the addresses of the tested zone's name servers map back to domain names.

**Implication:**

This is really more of an aesthetic issue than anything else. Query tools like nslookup and dig work better if your name server's address maps back to a domain name.

**Mitigation:**

If your name server's address doesn't map back to a domain name and you control the reverse-mapping zone the address is a part of, just add a PTR record for its address to the reverse-mapping zone. If someone else controls the reverse-mapping zone, ask them to add a PTR record for your name server.

<b>T004B</b>	<b>Check NS address PTR matches NS name</b>	<b>a.iana-servers.net. NS addresses have matching PTRs</b>	<b>green</b>
--------------	---	--	--------------

**Description:**

This test checks whether the addresses of a tested zone's name servers map back to the domain names of those name servers.

### Implication:

This is really more of an aesthetic issue than anything else. Query tools like nslookup and dig work better if your name server's address maps back to its domain name.

### Mitigation:

If your name server's address doesn't map back to a domain name and you control the reverse-mapping zone the address is a part of, just add a PTR record for its address to the reverse-mapping zone. If someone else controls the reverse-mapping zone, ask them to add a PTR record for your name server.

<b>T004B</b>	<b>Check NS address PTR matches NS name</b>	<b>b.jana-servers.net. NS addresses have matching PTRs</b>	<b>green</b>
--------------	---	--	--------------

### Description:

This test checks whether the addresses of a tested zone's name servers map back to the domain names of those name servers.

### Implication:

This is really more of an aesthetic issue than anything else. Query tools like nslookup and dig work better if your name server's address maps back to its domain name.

### Mitigation:

If your name server's address doesn't map back to a domain name and you control the reverse-mapping zone the address is a part of, just add a PTR record for its address to the reverse-mapping zone. If someone else controls the reverse-mapping zone, ask them to add a PTR record for your name server.

<b>T007A</b>	<b>Send SOA query</b>	<b>a.jana-servers.net. answers SOA query</b>	<b>green</b>
--------------	-----------------------	--	--------------

### Description:

This test sends each of the tested zone's authoritative name servers a nonrecursive query for the zone's SOA record. All of your name servers should respond authoritatively to such a query.

### Implication:

If any of your zone's name servers don't respond, or don't respond authoritatively to such a query, they're misconfigured. This will prevent other name servers from using them to resolve domain names in your zone and will lengthen the time it takes to resolve those domain names.

### Mitigation:

If the tested zone's authoritative name servers don't respond, there's probably an operational problem with those name servers. If your name servers return an error, such as SERVFAIL, that's an indication of a configuration error. Check your name servers' syslog output for a description of the error.

<b>T007A</b>	<b>Send SOA query</b>	<b>b.iana-servers.net. answers SOA query</b>	<b>green</b>
--------------	-----------------------	--	--------------

**Description:**

This test sends each of the tested zone's authoritative name servers a nonrecursive query for the zone's SOA record. All of your name servers should respond authoritatively to such a query.

**Implication:**

If any of your zone's name servers don't respond, or don't respond authoritatively to such a query, they're misconfigured. This will prevent other name servers from using them to resolve domain names in your zone and will lengthen the time it takes to resolve those domain names.

**Mitigation:**

If the tested zone's authoritative name servers don't respond, there's probably an operational problem with those name servers. If your name servers return an error, such as SERVFAIL, that's an indication of a configuration error. Check your name servers' syslog output for a description of the error.

<b>T007C</b>	<b>Check for AA bit</b>	<b>a.iana-servers.net. is authoritative for example.org</b>	<b>green</b>
--------------	-------------------------	---	--------------

**Description:**

This test sends each of the tested zone's authoritative name servers a nonrecursive query for the zone's SOA record and checks that the responses are authoritative (i.e., have the AA bit set in the DNS message header).

**Implication:**

Name servers that don't return authoritative responses are "lame," and can cause long resolution times and decreased resiliency.

**Mitigation:**

Authoritative name servers should return--no surprise here--authoritative responses to SOA queries for data in the zone. If they return a nonauthoritative response, that's an indication that the name server isn't configured as an authoritative for the zone, or that there's an error in the zone data file. Check your name server's syslog output for an error message. If your name servers return an error, such as SERVFAIL, that's also an indication of a configuration error.

<b>T007C</b>	<b>Check for AA bit</b>	<b>b.iana-servers.net. is authoritative for example.org</b>	<b>green</b>
--------------	-------------------------	---	--------------

**Description:**

This test sends each of the tested zone's authoritative name servers a nonrecursive query for the zone's SOA record and checks that the responses are authoritative (i.e., have the AA bit set in the DNS message header).

**Implication:**

Name servers that don't return authoritative responses are "lame," and can cause long resolution times and decreased resiliency.

### Mitigation:

Authoritative name servers should return--no surprise here--authoritative responses to SOA queries for data in the zone. If they return a nonauthoritative response, that's an indication that the name server isn't configured as an authoritative for the zone, or that there's an error in the zone data file. Check your name server's syslog output for an error message. If your name servers return an error, such as SERVFAIL, that's also an indication of a configuration error.

**T007D**
**Compare all SOA MNAME fields**
**SOA MNAME fields match**
**green**

### Description:

This test compares the MNAME fields of the SOA records returned from the tested zone's authoritative name servers. The MNAME field, which by convention contains the domain name of the zone's primary name server, should match on all authoritative name servers.

### Implication:

If your authoritative name servers are returning different answers, this could cause inconsistent resolver behavior, and could cause dynamic updates to be sent to different name servers.

### Mitigation:

If the MNAME field doesn't match on all of your zone's authoritative name servers and you haven't recently changed the field, your name servers might be out of synch. Check your secondary name servers' syslog output for errors indicating a failure to transfer the zone. Another possibility is that you run more than one primary for your zone. Active Directory-integrated zones have multiple primaries, for example.

**T007E**
**Compare all SOA RNAME fields**
**SOA RNAME fields match**
**green**

### Description:

This test compares the RNAME fields of the SOA records returned from the tested zone's authoritative name servers. The RNAME field, which by convention contains the email address of a technical contact for the zone, should match on all authoritative name servers.

### Implication:

If your authoritative name servers are returning different answers, this could cause inconsistent resolver behavior.

### Mitigation:

If the MNAME field doesn't match on all of your zone's authoritative name servers and you haven't recently changed the field, your name servers might be out of synch. Check your name servers' syslog output for errors indicating a failure to transfer the zone.

<b>T007F</b>	<b>Compare all SOA SERIAL fields</b>	<b>SOA SERIAL fields match</b>	<b>green</b>
--------------	--------------------------------------	--------------------------------	--------------

**Description:**

This test compares the serial numbers in the SOA records returned from the tested zone's authoritative name servers. The serial number should match on all authoritative name servers, except for brief inconsistencies after you've changed the zone data.

**Implication:**

If your authoritative name servers are returning different answers, this could cause inconsistent behavior on secondary name servers.

**Mitigation:**

If the serial numbers don't match on all of your zone's authoritative name servers and you haven't recently changed the field, your name servers might be out of synch. Check your name servers' syslog output for errors indicating a failure to transfer the zone. Another possibility is that you run more than one primary for your zone. Active Directory-integrated zones have multiple primaries, for example, and each may have a different serial number.

<b>T007G</b>	<b>Compare all SOA REFRESH fields</b>	<b>SOA REFRESH fields match</b>	<b>green</b>
--------------	---------------------------------------	---------------------------------	--------------

**Description:**

This test compares the REFRESH fields of the SOA records returned from the tested zone's authoritative name servers. The REFRESH field, which tells secondary name servers how often to check for changes to the zone on the primary, should match on all authoritative name servers.

**Implication:**

If your authoritative name servers are returning different answers, this could cause inconsistent behavior on secondary name servers.

**Mitigation:**

If the REFRESH field doesn't match on all of your zone's authoritative name servers and you haven't recently changed the field, it could be that your name servers are out of synch. Check your name servers' syslog output for errors indicating a failure to transfer the zone.

<b>T007H</b>	<b>Compare all SOA RETRY fields</b>	<b>SOA RETRY fields match</b>	<b>green</b>
--------------	-------------------------------------	-------------------------------	--------------

**Description:**

This test compares the RETRY fields of the SOA records returned from the tested zone's authoritative name servers. The RETRY field, which tells secondary name servers how often to check for changes to the zone on the primary after a refresh query has failed, should match on all authoritative name servers.

**Implication:**

If your authoritative name servers are returning different answers, this could cause inconsistent behavior on secondary

name servers.

### Mitigation:

If the RETRY field doesn't match on all of your zone's authoritative name servers and you haven't recently changed the field, it could be that your name servers are out of synch. Check your name servers' syslog output for errors indicating a failure to transfer the zone.

**T007I**

**Compare all SOA EXPIRE numbers**

**SOA EXPIRE fields match**

**green**

### Description:

This test compares the EXPIRE fields of the SOA records returned from the tested zone's authoritative name servers. The EXPIRE field, which tells secondary name servers how long they can answer queries without successfully refreshing the zone, should match on all authoritative name servers.

### Implication:

If your authoritative name servers are returning different answers, this could cause inconsistent behavior on secondary name servers.

### Mitigation:

If the EXPIRE field doesn't match on all of your zone's authoritative name servers and you haven't recently changed the field, it could be that your name servers are out of synch. Check your name servers' syslog output for errors indicating a failure to transfer the zone.

**T007J**

**Compare all SOA NEGTTL numbers**

**SOA NEGTTL fields match**

**green**

### Description:

This test compares the NEGTTL fields of the SOA records returned from the tested zone's authoritative name servers. The NEGTTL field, which tells remote name servers how long they can cache negative answers (e.g., NXDOMAIN and NODATA) from your zone's authoritative name servers, should match on all authoritative name servers.

### Implication:

If your authoritative name servers are returning different answers, this could cause inconsistent resolver behavior.

### Mitigation:

If the EXPIRE field doesn't match on all of your zone's authoritative name servers and you haven't recently changed the field, it could be that your name servers are out of synch. Check your name servers' syslog output for errors indicating a failure to transfer the zone.

**T007K**

**Examine SOA refresh**

**SOA refresh is 7200**

**green**

### Description:

This test checks whether the tested zone's REFRESH value falls within the range recommended by RFC 1912 (20m-

2h or 2h-12h).

### Implication:

REFRESH values outside of this range will either cause secondary name servers to check too frequently (less than 20 minutes) or too infrequently (more than 12 hours) for new zone data on their master name server.

### Mitigation:

If your zone's REFRESH value is outside the recommended range, you can set it to a more acceptable value by editing the SOA record on the zone's primary name server. Don't forget to increment the serial number! (On a zone that uses NOTIFY, however, the value you choose for REFRESH isn't that important.)

<b>T007L</b>	<b>Examine SOA retry</b>	<b>SOA retry/refresh ratio is 0.50</b>	<b>green</b>
--------------	--------------------------	--	--------------

### Description:

This test checks whether the tested zone's RETRY value falls within the range recommended by RFC 1912 (a fraction of the zone's REFRESH value).

### Implication:

RETRY values outside of this range will either cause secondary name servers to check too frequently or too infrequently for new zone data on their master name server.

### Mitigation:

If your zone's RETRY value is outside the recommended range, you can set it to a more acceptable value by editing the SOA record on the zone's primary name server. Don't forget to increment the serial number! (On a zone that uses NOTIFY, however, the value you choose for RETRY isn't that important.)

<b>T007M</b>	<b>Examine SOA expire</b>	<b>SOA EXPIRE meets RFC1912 suggestions</b>	<b>green</b>
--------------	---------------------------	---	--------------

### Description:

This test checks whether the tested zone's EXPIRE value falls within the range recommended by RFC 1912 (2w-4w).

### Implication:

EXPIRE values outside of this range will either cause secondary name servers to expire the zone too quickly or to continue responding for too long after failing to refresh the zone.

### Mitigation:

If your zone's EXPIRE value is outside the recommended range, you can set it to a more acceptable value by editing the SOA record on the zone's primary name server. Don't forget to increment the serial number!

<b>T007N</b>	<b>Examine SOA negttl</b>	<b>SOA minimum is 86400</b>	<b>yellow</b>
--------------	---------------------------	-----------------------------	---------------

**Description:**

This test checks whether the tested zone's NEGTTL value falls within a sane range (5m-1h).

**Implication:**

NEGTTL values outside of this range will either cause remote name servers to cache negative answers for too long, impairing your ability to modify your zone data, or will cause remote name servers to query your name servers too frequently, placing added load on them.

**Mitigation:**

If your zone's NEGTTL value is outside the recommended range, you can set it to a more acceptable value by editing the SOA record on the zone's primary name server. Don't forget to increment the serial number!

<b>T007O</b>	<b>Check SOA MNAME also in NS RR RDATA</b>	<b>SOA MNAME does not appear in NS RR RDATA</b>	<b>yellow</b>
--------------	--	---	---------------

**Description:**

This test checks whether the MNAME field in the tested zone's SOA record matches one of the name servers listed in the zone's NS records.

**Implication:**

If your zone's MNAME field isn't set to a name server in one of the zone's NS records, some dynamic updaters (particularly non-Microsoft updaters) may have trouble identifying the zone's primary name server and updating it. There's one case in which the MNAME shouldn't be set to the domain name of the zone's primary: If you use a hidden primary configuration-- which we can't detect--the MNAME field shouldn't contain the name of one of the name servers listed in the NS records.

**Mitigation:**

You can set the MNAME field by editing the SOA record on the zone's primary name server.

<b>T007P</b>	<b>Check syntax of SOA MNAME</b>	<b>MNAME 'dns1.icann.org' is valid</b>	<b>green</b>
--------------	----------------------------------	--	--------------

**Description:**

This test checks the syntax of the MNAME field of the tested zone's SOA record for validity. The MNAME field must contain a valid host name.

**Implication:**

If the MNAME field doesn't contain a valid host name, dynamic updates may not work, and secondary name servers may unnecessarily send NOTIFY messages to the zone's primary.

**Mitigation:**

Edit the zone's data file on the primary name server and change the MNAME field to a valid value.

**T007Q****Check syntax of SOA RNAME****RNAME 'hostmaster.icann.org' is valid****green****Description:**

This test checks the syntax of the RNAME field of the tested zone's SOA record for validity. It also checks whether the RNAME is set to the default value for Infoblox appliances. The RNAME field requires a special syntax: an Internet email address, but with a dot (".") substituted for the at-sign ("@").

**Implication:**

If the RNAME field doesn't contain a valid entry, or is uninitialized, it may not be possible for other DNS administrators to find the person responsible for management of your zone--you, presumably.

**Mitigation:**

Edit the zone's data file on the primary name server and change the RNAME field to a valid value.

**T010A****Try AXFR for zone****Zone transfer from a.iana-servers.net.:  
Response code from server: REFUSED****green****Description:**

This test tries to transfer the tested zone from its authoritative name servers.

**Implication:**

Allowing zone transfers from arbitrary IP addresses (like ours) increases your name servers' vulnerability to denial of service attacks and makes it easier for a would-be hacker to "map" your network. (Of course, in order to facilitate this tool's checks of zone data, you've probably opened up transfers from at least one of your zone's authoritative name servers. You can safely ignore that instance of this message as it applies to the name server you're allowing the tool to transfer from.)

**Mitigation:**

To lock down zone transfers, you can use the "allow-transfer" substatement in named.conf, like so:

```
options {
    allow-transfer { 10.0.0.1; };
};
```

Even better, you could use a TSIG key to secure zone transfers. For more information, see [this excerpt from the DNS & BIND Cookbook](#).

**T010A****Try AXFR for zone****Zone transfer from b.iana-servers.net.:  
Response code from server: REFUSED****green****Description:**

This test tries to transfer the tested zone from its authoritative name servers.

**Implication:**

Allowing zone transfers from arbitrary IP addresses (like ours) increases your name servers' vulnerability to denial of service attacks and makes it easier for a would-be hacker to "map" your network. (Of course, in order to facilitate this tool's checks of zone data, you've probably opened up transfers from at least one of your zone's authoritative name servers. You can safely ignore that instance of this message as it applies to the name server you're allowing the tool to transfer from.)

**Mitigation:**

To lock down zone transfers, you can use the "allow-transfer" substatement in named.conf, like so:

```
options {
    allow-transfer { 10.0.0.1; };
};
```

Even better, you could use a TSIG key to secure zone transfers. For more information, see [this excerpt from the DNS & BIND Cookbook](#).

<b>T011A</b>	<b>Test for open recursion</b>	<b>a.iana-servers.net. is not open to recursion</b>	<b>green</b>
--------------	--------------------------------	---	--------------

**Description:**

This test checks whether the name servers for the tested zone respond to recursive queries from arbitrary IP addresses.

**Implication:**

Allowing recursive queries from arbitrary IP addresses (like ours) increases your name servers' vulnerability to cache poisoning attacks and use in denial of service attacks against others.

**Mitigation:**

If your authoritative name servers don't serve any legitimate resolvers and aren't used as forwarders, you can disable recursion like this:

```
options {
    recursion no;
};
```

If your authoritative name servers are used by legitimate resolvers or are used as forwarders, you should consider splitting the recursive and authoritative functions between two sets of name servers. If you can't do that, at least use the "allow-recursion" substatement to restrict which clients get recursive name servers, like so:

```
options {
    allow-transfer { localnets; };
};
```

For more information, see [this excerpt from the DNS & BIND Cookbook](#).

**T011A****Test for open recursion****b.iana-servers.net. is not open to recursion****green****Description:**

This test checks whether the name servers for the tested zone respond to recursive queries from arbitrary IP addresses.

**Implication:**

Allowing recursive queries from arbitrary IP addresses (like ours) increases your name servers' vulnerability to cache poisoning attacks and use in denial of service attacks against others.

**Mitigation:**

If your authoritative name servers don't serve any legitimate resolvers and aren't used as forwarders, you can disable recursion like this:

```
options {
    recursion no;
};
```

If your authoritative name servers are used by legitimate resolvers or are used as forwarders, you should consider splitting the recursive and authoritative functions between two sets of name servers. If you can't do that, at least use the "allow-recursion" substatement to restrict which clients get recursive name servers, like so:

```
options {
    allow-transfer { localnets; };
};
```

For more information, see [this excerpt from the DNS & BIND Cookbook](#).

**T013A****Look for SPF TXT RRs****example.org has no TXT RRs****green****Description:**

This test checks whether the tested zone contains records supporting SPF, the Sender Policy Framework. The Sender Policy Framework uses DNS to let mail servers on the Internet authenticate email they receive. By examining TXT records attached to a domain name used in an email sender's address, a mail server can determine whether the mail server sending the email is authorized to send email from that domain name.

**Implication:**

Publishing SPF information makes it harder for someone to spoof email from your domain names.

**Mitigation:**

To set up SPF for your domain names, see the [SPF web site](#).

**T014A****Count number of MX records****Found 0 MX records****green**

**Description:**

This test simply counts the number of MX records the tested zone has. If the domain name of your zone is also an email destination, you should have an MX record for it. (If the domain name of your zone isn't an email destination, there's no point in adding an MX record for it, of course.)

**Implication:**

In most cases, listing only a single MX record (or multiple MX records, all with the same preference) is a good idea, as spammers frequently target backup mail exchangers.

**Mitigation:**

You can add or delete MX records by editing your zone's data file on the primary name server. Don't forget to increment the zone's serial number after you've made changes!

<b>T014D</b>	<b>Check for duplicate MX names</b>	<b>Found no MX records</b>	<b>yellow</b>
--------------	-------------------------------------	----------------------------	---------------

**Description:**

This test checks that no mail exchangers are listed more than once in the tested zone's MX records.

**Implication:**

A mail exchanger listed more than once doesn't add any redundancy and in fact can slow mail delivery.

**Mitigation:**

Remove duplicate MX records from your zone's data.

<b>T014E</b>	<b>Count unique MX preferences</b>	<b>Found 0 unique MX preference values ()</b>	<b>orange</b>
--------------	------------------------------------	---	---------------

**Description:**

This test counts the number of unique preference values in the tested zone's MX records.

**Implication:**

In most cases, listing only a single MX record (or multiple MX records, all with the same preference) is a good idea, as spammers frequently target backup mail exchangers.

**Mitigation:**

You can add or delete MX records by editing your zone's data file on the primary name server. Don't forget to increment the zone's serial number after you've made changes!

<b>T015C</b>	<b>Check for duplicate MX addresses</b>	<b>Found no MX records</b>	<b>yellow</b>
--------------	---	----------------------------	---------------

**Description:**

This test checks that no mail exchangers with the same address appear in the tested zone's MX records.

**Implication:**

A mail exchanger listed more than once doesn't add any redundancy and in fact can slow mail delivery.

**Mitigation:**

Remove duplicate MX records from your zone's data.

**T022A** Try an UPDATE **a.iana-servers.net. returned: REFUSED** green

**Description:**

This test attempts to dynamically update the tested zone.

**Implication:**

Allowing dynamic updates--especially from random addresses like the one this tool is running from--is an enormous security exposure. An updater has almost complete control over a zone: He can delete the entire contents of the zone, except for the SOA record and one NS record, and add completely different records.

**Mitigation:**

Apply access controls to dynamic updates to your zone, or if there are no authorized updaters, deny updates to the zone entirely. On a BIND name server, you can use the "allow-updates" substatement to restrict updates to certain addresses. For example:

```
zone "test.example" {
    type master;
    file "db.test.example";
    allow-update { 10.0.0.1; };
};
```

To deny updates entirely, you can use:

```
zone "test.example" {
    type master;
    file "db.test.example";
    allow-update { none; };
};
```

**T022A** Try an UPDATE **b.iana-servers.net. returned: REFUSED** green

**Description:**

This test attempts to dynamically update the tested zone.

**Implication:**

Allowing dynamic updates--especially from random addresses like the one this tool is running from--is an enormous security exposure. An updater has almost complete control over a zone: He can delete the entire contents of the zone, except for the SOA record and one NS record, and add completely different records.

### Mitigation:

Apply access controls to dynamic updates to your zone, or if there are no authorized updaters, deny updates to the zone entirely. On a BIND name server, you can use the "allow-updates" substatement to restrict updates to certain addresses. For example:

```
zone "test.example" {
    type master;
    file "db.test.example";
    allow-update { 10.0.0.1; };
};
```

To deny updates entirely, you can use:

```
zone "test.example" {
    type master;
    file "db.test.example";
    allow-update { none; };
};
```

**T023A****Look for Subdomains****No RRs for example.org: AXFR failed?****red**

### Description:

This test identifies delegated subdomains of the tested zone.

### Implication:

Unless those subdomains are explicitly excluded from testing, the tool will test them, too.

### Mitigation:

If you don't want particular delegated subdomains tested, list them on the tool's "Exceptions" tab.

**T029A****Check for different zone data with same serial number****Zone data appears to be different, with different serials****green**

### Description:

This test checks whether the zone data returned by different authoritative name servers is different, though the serial numbers returned by those authoritative name servers are the same. This indicates that someone modified zone data on the primary but forgot to increment the zone's serial number.

### Implication:

This can cause inconsistent answers depending on which authoritative name server you query.

**Mitigation:**

Increment the zone's serial number on the primary name server.

<b>T030A</b>	<b>Count hosts</b>	<b>Found 0 hosts in example.org</b>	<b>green</b>
--------------	--------------------	-------------------------------------	--------------

**Description:**

This test counts the number of A records in the zone. This is purely statistical.

**Implication:**

None.

**Mitigation:**

None.

<b>T032A</b>	<b>Check that domain name isn't repeated</b>	<b>Found 0 RRs with zone name repeated</b>	<b>green</b>
--------------	--	--	--------------

**Description:**

This test checks whether the domain name of the zone appears repeated in any domain names (for example, ns1.test.example.test.example).

**Implication:**

Repeated domain names like this are usually an indication of a missing trailing dot in the zone data file, like so:

```
test.example.    NS        ns1.test.example
```

If the default origin in the zone data file is test.example, the right side of the NS record expands to ns1.test.example.test.example.

**Mitigation:**

Find the offending record in the zone data file on the primary name server and add the missing trailing dot.

<b>T033A</b>	<b>Check for obsolete or deprecated RR types</b>	<b>No uncommon RR types found</b>	<b>green</b>
--------------	--	-----------------------------------	--------------

**Description:**

This test transfers a copy of the tested zone and identifies uncommon record types (all those except SOA, NS, A, PTR, MX, CNAME and TXT).

**Implication:**

While there's nothing wrong, per se, with using these record types, there's a good chance they aren't being used. Leaving them in the zone makes the zone larger, and therefore more resource-intensive to load and transfer.

**Mitigation:**

Remove any unused, uncommon record types.

<b>T034A</b>	<b>Check for wildcards</b>	<b>No wildcards found</b>	<b>green</b>
--------------	----------------------------	---------------------------	--------------

**Description:**

This test checks for the presence of wildcards in the tested zone.

**Implication:**

Wildcards have very limited uses, and can interact badly with search lists. Unless you're sure of what you're doing, you probably shouldn't use wildcards.

**Mitigation:**

Remove any unnecessary wildcards from your zone data.

<b>T035A</b>	<b>Check for unusual TTLs (very low, very high)</b>	<b>No unusual TTLs</b>	<b>green</b>
--------------	---	------------------------	--------------

**Description:**

This test checks for either very low or very high TTLs on records in the tested zone. "Very low" is currently defined as less than 30 seconds, while "very high" is more than one week.

**Implication:**

Except for special circumstances, such as load balancing, very low TTLs are unnecessary and can increase load on authoritative name servers. Using a TTL of zero can even prevent some older name servers from resolving a record. Very high TTLs will impair your ability to modify data.

**Mitigation:**

Increase or reduce TTLs on identified records as necessary.

**Name servers**

Name server	Potential problem	Configured correctly	Total cases completed
<a href="#">a.iana-servers.net.</a>	1	5	6
<a href="#">b.iana-servers.net.</a>	2	4	6

**Name server: a.iana-servers.net.**

<b>T005A</b>	<b>Fingerprint nameserver</b>	<b>a.iana-servers.net. is ISC BIND 9.2.0rc7 -- 9.2.2-P3</b>	<b>green</b>
--------------	-------------------------------	---	--------------

**Description:**

This test checks whether it's possible to fingerprint the tested zone's name servers (i.e., determine which name server software they run and its version). Almost every name server can be fingerprinted; the only question is how accurately. The tool we use for fingerprinting, fpdns, will occasionally get the make or model wrong.

**Implication:**

If your name server can't be fingerprinted or our tool guesses wrong, that's better for you because it'll be harder for a hacker to tailor an attack to your particular make and model of name server.

**Mitigation:**

None.

<b>T005B</b>	<b>Check fingerprint for vulnerable version</b>	<b>ISC BIND 9.2.0rc7 -- 9.2.2-P3</b>	<b>green</b>
--------------	---	--------------------------------------	--------------

**Description:**

This test cross-checks the version of the tested zone's authoritative name servers (as determined by test T005A) against ISC's Security Matrix. The cross-check isn't perfect, however. If the test flags yours as a vulnerable version of the BIND name server, verify that assessment against the matrix yourself [here](#).

**Implication:**

Running a vulnerable or outdated name server implementation is very dangerous. A hacker could capitalize on a vulnerability to gain control of your name server, and possibly use your name server as a stepping stone to attack your other hosts. He could publish bogus data, directing your users and customers to your competition or to a fake copy of your web site or mail server, where their data could be harvested.

**Mitigation:**

If you find that your name server is vulnerable, upgrade to a current version as soon as possible.

<b>T006A</b>	<b>Send VERSION.BIND query</b>	<b>a.iana-servers.net. returns "9.2.1"</b>	<b>yellow</b>
--------------	--------------------------------	--	---------------

**Description:**

This test checks whether it's possible to fingerprint the tested zone's name servers (i.e., determine which name server software they run and its version) by sending them queries for a TXT record attached to the pseudo-domain name version.bind in the CHAOSNET class. BIND name servers, unless otherwise configured, return their version as part of the response to these queries.

**Implication:**

If your name server can be fingerprinted using this method, it's that much easier for a hacker to determine its vulnerabilities and then tailor an attack to your particular make and model of name server.

**Mitigation:**

Configuring most name servers not to respond to these queries is easy. On most BIND 8 and 9 name servers, you can add a "version" substatement to your name server's "options" statement in named.conf, like so:

```
options {
    version "None of your business";
};
```

On BIND 9.3.x name servers, you can also use:

```
options {
    version none;
};
```

For more information on these and other options, see [this excerpt from the DNS & BIND Cookbook](#).

**T007B****Measure response time****a.iana-servers.net. responded in 28 msec****green****Description:**

This test sends each of the tested zone's authoritative name servers a query and times the responses. If you're performing the test from your own network and the authoritative name servers aren't too distant, the response times should be low-- generally, less than 100ms.

**Implication:**

Longer response times mean longer name resolution times and reduced performance for applications.

**Mitigation:**

If you find one or more of your name servers are responding slowly, you need to determine why before you can address the problem. Is the name server simply a long way away from the querier? Is the name server overloaded? You might check how many queries it's receiving per second or how much CPU it's using. For details on how to measure query load on a name server, see [this excerpt from the DNS & BIND Cookbook](#).

**T008A****Send TCP-based SOA query****a.iana-servers.net. TCP succeeded****green****Description:**

This test checks whether the tested zone's authoritative name servers respond to a TCP-based query for the zone's SOA record. While DNS messages (queries and responses) are normally sent over UDP, there are occasions when TCP is used. For example, if one of your zone's authoritative name servers can't fit all of the records in a response into a UDP-based DNS message, it will make the response as truncated. The querier may then retry the query over TCP.

**Implication:**

Not serving TCP-based queries will cause your name server to fail to answer in seemingly random situations, such as when an answer exceeds a certain size.

**Mitigation:**

If one or more of your name servers aren't responding to TCP-based queries, it's probably due to access controls on a router or firewall. You can adjust your router's or firewall's access controls to allow TCP connections to the DNS port, port 53, on your name servers.

<b>T012A</b>	<b>Test for EDNS0 support</b>	<b>a.iana-servers.net. supports EDNS0</b>	<b>green</b>
--------------	-------------------------------	---	--------------

#### Description:

This test checks whether the tested zone's authoritative name servers respond to a EDNS0 query for the zone's SOA record. EDNS0 is used by modern name servers to carry large payloads over UDP. Traditionally, UDP-based DNS messages have been limited to 512 bytes. With EDNS0, UDP-based DNS messages can be as large as 4KB. As we begin storing more complex records in DNS to support new applications such as SPF, DKIM and ENUM, EDNS0 support will be increasingly important.

#### Implication:

Not supporting EDNS0 will make it difficult, or at least more costly, for your name servers to support new DNS applications such as SPF, DKIM and ENUM.

#### Mitigation:

If your name servers don't support EDNS0, the only solution is to upgrade to a name server that does.

**Name server: b.iana-servers.net.**

<b>T005A</b>	<b>Fingerprint nameserver</b>	<b>b.iana-servers.net. is ISC BIND 9.2.3rc1 -- 9.4.0a0</b>	<b>green</b>
--------------	-------------------------------	--	--------------

#### Description:

This test checks whether it's possible to fingerprint the tested zone's name servers (i.e., determine which name server software they run and its version). Almost every name server can be fingerprinted; the only question is how accurately. The tool we use for fingerprinting, fpdns, will occasionally get the make or model wrong.

#### Implication:

If your name server can't be fingerprinted or our tool guesses wrong, that's better for you because it'll be harder for a hacker to tailor an attack to your particular make and model of name server.

#### Mitigation:

None.

<b>T005B</b>	<b>Check fingerprint for vulnerable version</b>	<b>ISC BIND 9.2.3rc1 -- 9.4.0a0</b>	<b>green</b>
--------------	---	-------------------------------------	--------------

#### Description:

This test cross-checks the version of the tested zone's authoritative name servers (as determined by test T005A) against ISC's Security Matrix. The cross-check isn't perfect, however. If the test flags yours as a vulnerable version of the BIND name server, verify that assessment against the matrix yourself [here](#).

**Implication:**

Running a vulnerable or outdated name server implementation is very dangerous. A hacker could capitalize on a vulnerability to gain control of your name server, and possibly use your name server as a stepping stone to attack your other hosts. He could publish bogus data, directing your users and customers to your competition or to a fake copy of your web site or mail server, where their data could be harvested.

**Mitigation:**

If you find that your name server is vulnerable, upgrade to a current version as soon as possible.

<b>T006A</b>	<b>Send VERSION.BIND query</b>	<b>b.iana-servers.net. returns "9.2.3"</b>	<b>yellow</b>
--------------	--------------------------------	--	---------------

**Description:**

This test checks whether it's possible to fingerprint the tested zone's name servers (i.e., determine which name server software they run and its version) by sending them queries for a TXT record attached to the pseudo-domain name version.bind in the CHAOSNET class. BIND name servers, unless otherwise configured, return their version as part of the response to these queries.

**Implication:**

If your name server can be fingerprinted using this method, it's that much easier for a hacker to determine its vulnerabilities and then tailor an attack to your particular make and model of name server.

**Mitigation:**

Configuring most name servers not to respond to these queries is easy. On most BIND 8 and 9 name servers, you can add a "version" substatement to your name server's "options" statement in named.conf, like so:

```
options {
    version "None of your business";
};
```

On BIND 9.3.x name servers, you can also use:

```
options {
    version none;
};
```

For more information on these and other options, see [this excerpt from the DNS & BIND Cookbook](#).

<b>T007B</b>	<b>Measure response time</b>	<b>b.iana-servers.net. responded in 164 msec</b>	<b>yellow</b>
--------------	------------------------------	--	---------------

**Description:**

This test sends each of the tested zone's authoritative name servers a query and times the responses. If you're performing the test from your own network and the authoritative name servers aren't too distant, the response times should be low-- generally, less than 100ms.

**Implication:**

Longer response times mean longer name resolution times and reduced performance for applications.

**Mitigation:**

If you find one or more of your name servers are responding slowly, you need to determine why before you can address the problem. Is the name server simply a long way away from the querier? Is the name server overloaded? You might check how many queries it's receiving per second or how much CPU it's using. For details on how to measure query load on a name server, see [this excerpt from the DNS & BIND Cookbook](#).

**T008A****Send TCP-based SOA query****b.iana-servers.net. TCP succeeded****green****Description:**

This test checks whether the tested zone's authoritative name servers respond to a TCP-based query for the zone's SOA record. While DNS messages (queries and responses) are normally sent over UDP, there are occasions when TCP is used. For example, if one of your zone's authoritative name servers can't fit all of the records in a response into a UDP-based DNS message, it will make the response as truncated. The querier may then retry the query over TCP.

**Implication:**

Not serving TCP-based queries will cause your name server to fail to answer in seemingly random situations, such as when an answer exceeds a certain size.

**Mitigation:**

If one or more of your name servers aren't responding to TCP-based queries, it's probably due to access controls on a router or firewall. You can adjust your router's or firewall's access controls to allow TCP connections to the DNS port, port 53, on your name servers.

**T012A****Test for EDNS0 support****b.iana-servers.net. supports EDNS0****green****Description:**

This test checks whether the tested zone's authoritative name servers respond to a EDNS0 query for the zone's SOA record. EDNS0 is used by modern name servers to carry large payloads over UDP. Traditionally, UDP-based DNS messages have been limited to 512 bytes. With EDNS0, UDP-based DNS messages can be as large as 4KB. As we begin storing more complex records in DNS to support new applications such as SPF, DKIM and ENUM, EDNS0 support will be increasingly important.

**Implication:**

Not supporting EDNS0 will make it difficult, or at least more costly, for your name servers to support new DNS applications such as SPF, DKIM and ENUM.

**Mitigation:**

If your name servers don't support EDNS0, the only solution is to upgrade to a name server that does.

© 2006, 2007 Infoblox Inc. All rights reserved. All registered trademarks are property of their respective owners.