

Re: Some DNS server names will not resolve using internal servers

## Re: Some DNS server names will not resolve using internal servers

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2006-12/msg00016.html>

---

- *From:* Brillmike <[brillmike@xxxxxxxxxx](mailto:brillmike@xxxxxxxxxx)>
  - *Date:* Tue, 28 Nov 2006 13:43:15 -0800
- 

Thanks for expalining the DNAME information. Maybe that is not the issue.

I have done all the nslookup commands. All of our external ISP DNS fporwarders return the CNAMEs for www.microsoft.com. When we NSLookup to our internal servers we get "can't find www.microsoft.com: server failed"

nothing is logged on the DNS server application logs.

I tried from workstations and from the DNS servers. No luck.

If i by pass the local DNS servers from the workstations I can get to www.microsoft.com. So i think that would elimanate a local workstation issue?

Is there a trace i could do on the DNS server to tell me what is happening?

I am going to schedule a reboot to the DNS servers for the weekend.

"Herb Martin" wrote:

"Brillmike" <[brillmike@xxxxxxxxxx](mailto:brillmike@xxxxxxxxxx)> wrote in message  
[news:371587CE-72FF-4E29-A74B-6DF3D747970C@xxxxxxxxxxxxxxxxxxxxx](mailto:news:371587CE-72FF-4E29-A74B-6DF3D747970C@xxxxxxxxxxxxxxxxxxxxx)

I was thinking maybe DNAME. Which is redirection to a DNS tree...  
<http://www.ietf.org/internet-drafts/draft-ietf-dnsect-rfc2672bis-dname-00.txt>  
We do not have any external zones set up and forward all request to our ISP's, which work fine.

That isn't even a standard so it is unlikely unless you have some specific information that makes you believe that your ISP is engaged in such things.

Even then it would likely be a hack/compromise of the ISPs DNS by some employee or outside attacker (e.g., an MS hater.)

Re: Some DNS server names will not resolve using internal servers

I think this could explain why it only happens to WWW.microsoft.com, not SUPPORT.microsoft.com

Not really, since the DNAME would typically be used to redirect all of Microsoft.com. Only a CNAME would be needed for a specific name like "support.microsoft.com".

DNAME do in fact redirect queries from zone A to zone B with the specific host name being prepending to the latter (i.e., B) instead of the original (i.e., A).

I am not sure how to fix it, I think it is a bug in 2003 DNS. I saw the HOTFIX article as mentioned in this thread but want to confirm that this is the issue.

What problem have you specifically identified?  
(I don't actually believe, or at least don't understand, that you have identified any specific problem.)

Until you can show the actual NSLookup responses to specific servers to be giving different answers you haven't even approach the level of explicitness you need to declare a bug.

[I am saying this as someone who has discovered significant bugs in Cisco, Netware, IBM, Microsoft, and Apple software that had previously gone unreported -- almost always I find that the problems are NOT bugs and these were all the exceptions.]

I cant find a virus/trojan and all other sites appear to be working.

What ISP and which DNS servers are you using?  
We can try to check them directly.

It might be interesting for you to learn (or discover for yourself) that Support.Microsoft.com is a completely different ZONE from Microsoft.com, and that this zone is managed by an entirely (apparently) different set of servers, perhaps at a completely different company.

msft.net vs. akamai.com

nslookup -q=microsoft.com  
nslookup -q=soa support.microsoft.com

Re: Some DNS server names will not resolve using internal servers

(you will actually discover this is a CNAME and that you must re-issue the request as:)

```
nslookup -q=soa support.microsoft.akadns.net
```

Here is an article I found too might be some interest. I will keep looking for an answer. <http://cr.yp.to/djbdns/kill6.html>. Hope someone at MS can help too.

I suggest you very carefully perform all of the required NSLookup tests (that I have been suggesting all along and that would derive from the results of those tests) and post that explicitly.

You must include tests from the command line of the actual DNS server (to prove that there is not some weird interaction for just this server) as well as the full list of Forwarders and whether "Do Not use Recursion" is checked or not.

You might also consider using Debug logging to document the requests and responses.

Proving a bug (by eliminating all of the other variables) is actually quite involved.

--

Herb Martin, MCSE, MVP  
Accelerated MCSE  
<http://www.LearnQuick.Com>  
[phone number on web site]

"Herb Martin" wrote:

"Brillmike" <brillmike@xxxxxxxx> wrote in message  
<news:CA651CFC-5640-4195-947B-DC2B3E562550@xxxxxxxxxxxxxxxxxxxx>

Could this have something do do with a  
DNAME. I have run across an  
article  
concerning a HOTFIX...KB920162.

Do you mean CNAME?

Re: Some DNS server names will not resolve using internal servers

Why would you have ANY records for the external sites?

If you do have the zone for any external sites then your (internal) version of that zone must be absolutely correct.

--

Herb Martin, MCSE, MVP  
Accelerated MCSE  
<http://www.LearnQuick.Com>  
[phone number on web site]

I see DNS events, informational, for Event ID 5504 on myu domain controller.

They look harmless but look related to me doing nslookups on the domain names that fail. Both of these names seem to have multiple IP addresses associated with the name....no a typical cname.

Can you shed some light, am i on to something?

"Herb Martin" wrote:

"Brillmike"  
<brillmike@xxxxxxxxxx>  
wrote in message  
<news:DF3F6728-90EF-4312-BA00-AD24BF258691@xxxxxxxxxxxxxxxxxxxx>

www for  
microsoft is  
working  
again. I did  
not change  
anything  
but  
now  
the  
site is  
coming up  
fine.

BUT...LOGIN.gsionline.com

Re: Some DNS server names will not resolve using internal servers

```
is still not
working.
www.gsonline.com
is.
When
i
do the
nslookup on
our ISP
server i get
this.
Address:
66.28.0.45
Non-authoritative
answer:
Name:
login.gsonline.com
Addresses:
167.68.27.53,
167.68.27.54,
167.68.27.55,
167.68.27.11
```

So the ISP is working and  
can be reached.

```
ON our own
DNS server,
which have
the above
addresses as
FORWARDERS.
I
get
this
response.
```

```
Address:
10.10.0.202
```

```
DNS
request
timed out.
timeout was
2 seconds.
*** Request
to
sfdc1.howardrice.local
timed-out
```

Re: Some DNS server names will not resolve using internal servers

Your server didn't answer.  
You should play with  
timeout value to ensure it is  
true failure and not just  
slow:

```
nslookup -time=20  
login.gsonline.com  
10.10.0.202
```

[You should also try these  
FROM the actual Server's  
command line too -- this  
will tell you if this is just  
some problem with THIS  
server failing to reach a  
particular resolution which  
the client can resolve  
directly.]

But the  
forwarding  
is working  
for  
everything  
else  
(www.microsoft.com  
is  
sketchy)  
C:\Documents  
and  
Settings\mab>nslookup  
www.gsonline.com  
10.10.0.202  
Server:  
sfdc1.howardrice.local  
Address:  
10.10.0.202

Non-authoritative  
answer:  
Name:  
www.gsonline.com  
Addresses:  
167.68.27.18,  
167.68.27.47

C:\Documents

Re: Some DNS server names will not resolve using internal servers

```
and
Settings\mab>nslookup
www.gsionline.com
10.10.0.203
Server:
sfdc2.howardrice.local
Address:
10.10.0.203
```

```
Non-authoritative
answer:
Name:
www.gsionline.com
Addresses:
167.68.27.47,
167.68.27.18
```

```
We have
not
rebooted the
DNS server
yet. Could
this be a
caching
issue.
I
see entries
for
gsionline,
but nothing
the
references
LOGIN.gsionline.com
```

Not likely a caching issue since the resolution itself is not failing (the DNS server is TIMING OUT completely).

So you are saying that if you change nothing but the "login.gsionline.com" name to something else your NSLookup commands work when they fail with Login name against internal servers?

That is very goofy.

Re: Some DNS server names will not resolve using internal servers

Re: Some DNS server names will not resolve using internal servers

I might (eventually) reboot the server(s) but this is not something that is usually necessary or even that useful.

You can check the cache in the MMC by enabling "Advanced" view. Cache will show as a pseudo zone tree.

--

Herb Martin, MCSE, MVP  
Accelerated MCSE  
<http://www.LearnQuick.Com>  
[phone number on web site]

"Herb  
Martin"  
wrote:

"Brillmike"  
<brillmike@xxxxxxxxxx>  
wrote  
in  
message  
<news:A5F49CB3-FA14-4EFA-8C96-F587A2788AC2@xx>

We  
have  
two  
W2003  
AD/DNS  
server  
replicating.  
From  
our  
client  
XP  
machines  
I  
can

Re: Some DNS server names will not resolve using internal servers

go  
to  
support.microsoft.com  
but  
not  
WWW.microsoft.com.  
I  
can  
go  
to  
WWW.gsionline.com  
but  
not  
LOGON.gsionline.com.  
We  
use  
forwarding  
so  
all  
internal  
machines  
are  
pointing  
to  
our  
internal  
DNS  
server.  
We  
do  
not  
seem  
to  
have  
any  
issue  
with  
any  
other  
server  
names,  
just  
WWW  
for  
microsft.com  
and  
LOGON  
for  
gsionline.com.

Re: Some DNS server names will not resolve using internal servers

Ok,  
then  
somewhere  
those  
(2)  
records  
are  
being  
overridden  
or  
picked  
up  
(hosts  
file,  
explicit  
zones,  
trojan/virus,  
etc.)

What  
to  
do?

When  
you  
face  
such  
issues  
the  
first  
thing  
to  
do  
is  
to  
test  
each  
DNS  
server  
involved  
**EXPLICITLY**  
(from  
the  
clients):

nslookup  
www.Microsoft.com  
ISP.DNS.Server.IP

Re: Some DNS server names will not resolve using internal servers

nslookup  
www.Microsoft.com  
Internal.DNS.Server.IP

(Do  
the  
first  
one  
for  
EACH  
and  
EVERY  
internal  
DNS  
server.)

If  
both  
of  
these  
work,  
then  
likely  
you  
have  
something  
(screwy)  
in  
a  
local  
Hosts  
file  
(%systemroot%\system32\  
drives\etc\hosts).  
Such  
MIGHT  
be  
put  
there  
by  
a  
malicious  
program  
or  
user  
who  
hates  
MS.

Re: Some DNS server names will not resolve using internal servers

BTW:  
if  
i  
set  
the  
client  
to  
bypass  
the  
local  
DNS  
servers  
and  
resolve  
to  
the  
DNS  
server  
we  
forward  
lookup  
to,  
then  
i  
can  
resolve  
the  
addresses.

You  
must  
never  
do  
this  
(except  
for  
test  
purposes)  
--  
internal  
machines  
must  
use  
STRICTLY  
the  
internal  
DNS  
servers  
which  
can

Re: Some DNS server names will not resolve using internal servers

resolve  
both  
internal  
and  
external  
names.

--

Herb  
Martin,  
MCSE,  
MVP  
Accelerated  
MCSE  
<http://www.LearnQuick.Com>  
[phone  
number  
on  
web  
site]

Thanks,  
Mike