

Re: DNS Cache corruption?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2008-06/msg00012.html>

- *From:* "Herb Martin" <news@xxxxxxxxxxxxxxxx>
 - *Date:* Mon, 2 Jun 2008 23:37:09 -0500
-

"infinigtuy" <derek@xxxxxxxx> wrote in message
news:A45BB2F1-A77C-4E40-865B-D991F66142B5@xxxxxxxxxxxxxxxx

Sorry, You're right, after reading through.. it is a bit vague.

The plan is to remove those, and implement MSDNS, which we already have in place for our ionaglobal.com zone(for exchange). We just consolidated all of our NT4 domains to ionaglobal, so the next logical step is to get all of our workstations/servers that are using the old DNS to use the new DNS.

The plan will be to have two stub zones. One here(10.65.6.2 eventually) and one in dublin(10.2.2.49). These stub zones will point to the various DC's(4 in waltham, and 2 in dublin) for DNS. Overall there'll be 8 dns servers(2 stubs, and 6 DC's/DNS).

What's the point of all these stubs? Don't you have DCs in those locations?

None of this has much to do in all likelihood with your subject line.

The reason that amer-dns1 is using secondary zones is I'm not cutting the entire company over to MSDNS in one swoop. I'm going to do waltham first, then dublin a few weeks later. I'd rather only break half the company if something goes wrong. The need for the secondaries will be to do local name resolution for the zones Dublin hosts, rather than setting up a bunch of zone forwards.. eventually all of the zones will be ADI zones, and the only zones that amer-dns1(stub server) will host.. will be stub zones.

Microsoft DNS just works. You are likely experiencing some problem from OUTSIDE, e.g., whoever is giving you AOL and CNN, not your DNS servers or those that are authoritative for those zones.

Re: DNS Cache corruption?

We will have a single forest/single domain.

The use of the stub servers will be to allow the DNS server to be re-iped when it's time to go into production without having to promote/create a new DC that will inherit that IP.. none of the clients will be pointing to the other DNS servers so I figure the stub will be a constant, always on central point to distribute the load.

You aren't really focusing on one problem here.

When Ace asked for a clear infrastructure he doesn't care about YOUR ZONES.

Your problem is with EXTERNAL ZONES.

Resolving your own zones is a nearly separate job from resolving the INTERNET.

You should ALWAYS think of these, design these, troubleshoot these as separate jobs even if the same server(s) do them.

There will be a DNS/DC at each major location. That I'm not worried about yet.

None of this matters to your current problem.

re: firewall. We use a checkpoint firewall. I don't know if it supports EDNS0.. I know that there was a bug within our current DNS system where when dns caching was enabled dns would eventually crash, so that DNS admin just turned off caching... the product is full of bugs which is why we're moving off of it.

I guess the thing I just don't understand is what causes the behavior to happen. Why cnn.com? Why aol.com in my experience a month ago, and why

Where is it happening?

You need to "Nslookup" and/or view the caches with the MMC until you find the FIRST (most outside) culprit.

If I ask YOU a question, and get a wrong answer, then I pass that wrong answer on to someone else the problem is not with me (by analogy.)

Do this (when it happens):

nslookup www.cnn.com IP.DNS.Server.Local

Re: DNS Cache corruption?

Re: DNS Cache corruption?

nslookup www.cnn.com IP.Local.Forwards.To

Etc, until you find the FURTHEST outbound server with the wrong answer.

If you find a RECURSIVE (non-forwarding) DNS Server in the list then you have to work through from the ROOT down, the same way that recursive server does it until you find the culprit.

Isolate. Isolate. Isolate.

Probably are easy to solve (usually) but sometimes difficult to locate.

when the cache is cleared does it work fine, and continue to work fine with the new cached record? Unfortunately I don't have details of the ttl's or anything for the buggy records since I had to clear the cache earlier today. Maybe the firewall thing is something to look into but I'm not sure if that's what's causing the woes.

Your DNS infrastructure description is a bit confusing and doesn't provide enough specific info.

Can you elaborate on what the following sentence means?

"I've gotten internal IT on to my
DNS server, "

Are the "other" DNS servers, such as Amer-DNS1, domain controllers? If so, be careful to manually create a zone that is AD Integrated, especially if the zone is in the same Replication Scope the domain controller is part of.

Do you have one domain in one forest or a multi-domain forest?

Not sure why you are using stubs and secondaries, that is if these other DNS servers are truly domain controllers? It can lead to DNS issues.

Is there a DC at each location? If so, it would be beneficial for them to be DNS servers.

What type of firewall do you have? Maybe it doesn't support EDNS0. Check your documentation on how to enable it. Lack of EDNS0 support will lead

Re: DNS Cache corruption?

to failed resolution of zone with large data, that is above 512 bytes. You can check if your firewall supports EDNS0. Use nslookup. Query for the sites you say you cannot resolve. Then change it to TCP (by using the set vc command). If it resolves, then it's an EDNS0 issue.

By legacy methods, DNS query traffic uses UDP. Now on the response side, if it is larger than 512 bytes, legacy method (non-EDNS0) will revert the response to TCP. If DNS supports EDNS0, which Windows 2003 does, it believes there is no reason to revert, but then what happens is the firewall will block the traffic if it cannot support a DNS UDP response packet larger than 512 bytes.

If you have a PIX, the command is:
protocol fixup dns 1280

—

Regards,
Ace

This posting is provided "AS-IS" with no warranties or guarantees and confers no rights.

Ace Fekay, MCSE 2003 & 2000, MCSA 2003 & 2000, MCSE+I, MCT,
MVP Microsoft MVP – Directory Services
Microsoft Certified Trainer

For urgent issues, you may want to contact Microsoft PSS directly. Please check <http://support.microsoft.com> for regional support phone numbers.

Infinite Diversities in Infinite Combinations