

Re: Questions on putting up a new DNS server.

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.dns/2005-04/msg00211.html>

- *From:* "Herb Martin" <news@xxxxxxxxxxxxxxxx>
 - *Date:* Sun, 10 Apr 2005 22:00:06 -0500
-

"Bill-MT" <BillMT@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:CECB098B-0AC2-4F8C-87EF-6407079A5FDD@xxxxxxxxxxxxxxxx
> First, Thanks to both of you for responding. And Herb, it's good to see
you
> are still 'on-board' I really appreciated the answers you gave me for
> questions I submitted last fall.

My pleasure.

> Below is a summary of my site, relative to the answers you have already
> given me.
>
> Root Domain: contains the DC's Root_X, Root_Y, and Root_Z. however,
since
> no AD-DNS exists in the root domain itself, none of these DC's share in
the
> Root domain AD-zone info.

Why do you mention them if they aren't involved?

> These DC's however, are clients of the User domain
> AD-DNS servers DC_A and DC_B, so therefore they do successfully populate
> their 'serv' records into the AD-integrated Root domain housed on servers
> DC_A and DC_B. There are no other servers or clients in the Root domain.

It is not illegal but very odd, and probably not
the more reliable, for you to put the AD-integrated
zone for ONE Domain on a different domains DCs.

Especially in Win2000 where there is no cross domain
replication for DNS.

> User Domain: servers DC_A and DC_B are the only AD-DNS servers in the user
> domain (or really the site). However, the other non-DNS DC's in the User
> domain (DC_D and DC_E) do have copies of the User domain via AD
replication
> from their AD-DNS counter-parts. Member server Serv_C is a cache_only DNS
> server which is set to refer to DC_A and DC_B for answers for Root and

Re: Questions on putting up a new DNS server.

User

- > domain questions. All servers (both DC's and member) are clients of DC_A and
- > DC_B. Most desktops are also clients of DC_A and DC_B, however, some
- > desktops are clients of Serv_C and DC_B (in that order).

Why are you doing something so complicated? Even the explanation above is hard to figure out.

- > Servers DC_A and DC_B and Serv_C are also the WINS servers for the site,
- > with servers DC_B and Serv_C replicating registrations to/from DC_A All
- > site servers and desktops are configured to list at least two of these
- > servers in their Wins configuration.
- >
- > Please comment on the above summary if I have mis-spoken your responses in
- > any way.

I would simplify it. Make the DCs in the root domain their own DNS servers -- integrate them into AD.

Make the DCs in the child domain their own DNS -- integrate them.

Make the DNS servers in the child domain into DNS Secondaries for the root. (You have more choices in Win2000 when you finally upgrade.)

- > Additional Questions, based on your previous responses {please correct where
- > I'm wrong}.
- >
- > 1) Can you {very briefly because you have covered this already} explain how
- > a desktop uses the above infrastructure (who they talk to) when they need to
- > do intra-forest DNS work.

Well, with my replacement (right above) you can point child DNS clients at their own DNS where they will find their own domain info directly and which can find the parent for them because it will hold a secondary.

- > Basically I'd like to make sure I really
- > understand how clients work, who they talk with in my situation, for example,
- > how would a client configured to use DC_A differ from a client configured to
- > use Serv_C?

It isn't how clients work, so much as how their DNS servers work.

Re: Questions on putting up a new DNS server.

Re: Questions on putting up a new DNS server.

Clients ask a DNS Server for resolution — it is up to that DNS server to FIND EVERYTHING the client might ever need:

Domain, child or parent domains, sibling domains, and even disjoint trees (different names) — and of course the Internet for most people.

> 2) Since all member Servers are either W2K or W2K3. And 97% (there are
> still a handful of 9x machines and samba users) of all Desktops are either
> W2K or XP — when is Wins used in my infrastructure. Should we stop
> configuring our servers and desktops with Wins, will this force everything
to
> use DNS.

No, you will need WINS if you have multiple subnets.

Almost no one can forego NetBIOS resolution, and NetBIOS resolution requires WINS (practically) for multiple subnets.

> What about browse groups and network neighborhood – how does this
> stuff get populated under a DNS-only environment.

It does NOT — you need WINS server.

> Will an W2K3-AD
> infrastructure be any different {when is Wins going away}.

2010 or a bit later probably. <grin>

(It isn't going away for the foreseeable future.)

> 3) Sounds like I should wait to worry about putting any AD-DNS servers
into
> my Root domain until after I move to W2K3-AD because then the zones will
not
> have use domain specific AD-replication. Therefore I'll put the new
server
> (replacing DC_A) back into the User domain.

If it works you can wait but I don't like it.

It is something of a style issue but I can think of a bunch of ways it will go bad that aren't necessary if you clean up the design.

Have the DNS-DCs hold the zones from the same domain. Have the other domain(s) hold secondaries for all other zones they cannot reach by recursion.

Re: Questions on putting up a new DNS server.

Re: Questions on putting up a new DNS server.

With multiple DNS trees every DNS server must also hold EACH tree root as a Secondary --- if you wish to forward or recurse the Internet.

- > 4) Right now I only have the default site (location) configured. If I add
a
> new site location { which will include a remote DC in the Root domain and
a
> remote DC in the User domain} what are your recommendations for DNS at
that
> remote site {should it be AD-integrated on one of these new DC's or
> cache-only on a member server, or nothing - no local dns server}.

This is the reason that I want you to simplify --- DNS on DC from same domain. If you need a local DC, you need it to have DNS (and on it is the generally best place.)

- > 5) Finally, slightly off the subject, but since I am in the process of
> building a new AD-DNS (DC) server, do you believe it is good practice to
add
> Anti-Virus software to Domain Controllers. If you do believe it is good
> policy, do you do so with any caveats.

If you can do it without messing them up, AND it is even remotely possible that a DC would become infected (which it is in almost all cases.)

> Thanks in advance for your time and your answers. - Bill

You could call me if you get confused.... phone on web site:
LearnQuick.Com

.

• *Follow-Ups:*

- ◆ *Re: Questions on putting up a new DNS server.*
◇ From: Bill-MT

• *References:*

- ◆ *Questions on putting up a new DNS server.*
◇ From: Bill-MT
- ◆ *RE: Questions on putting up a new DNS server.*
◇ From: Bill-MT

- Prev by Date: *RE: Questions on putting up a new DNS server.*
- Next by Date: *change subnet*
- Previous by thread: *RE: Questions on putting up a new DNS server.*
- Next by thread: *Re: Questions on putting up a new DNS server.*

Re: Questions on putting up a new DNS server.

Re: Questions on putting up a new DNS server.

- Index(es):

- ◆ *Date*

- ◆ *Thread*