

# Re: Windows 2003 DNS Setup for Sub-Domain off of Root

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2005-02/0104.html>

---

**From:** Roger Abell (*mvpNOSpam\_at\_asu.edu*)

**Date:** 01/29/05

Date: Sat, 29 Jan 2005 15:46:18 -0700

Fundementally, Herb's comment is correct, that admins do need to be trusted to do the right thing.

However, you can design it so that they have to go out of their way to do some of the wrong things

some comments are inlined below . . .

--

Roger

"Mike Graves" <MikeGraves@discussions.microsoft.com> wrote in message news:467AE4D9-D4E4-47E1-B330-DD73CACB1C83@microsoft.com...

> Roger;

>

> That is correct; I do not want the admins in each domain to be able to alter

> dns in any other zone than the one that is assigned to them. I plan on

> delegating each sub-domains zone from the root domain. I then will create

> the primary zones in the sub-domains.

>

> Questions:

>

> -Since I have the delegation of the sub-domains on the root zone, I do not

> need secondary zones of the sub-domains on the root server. Would it make

> sense to put secondary zones of the sub-domain zones on the root server

for

> fault tolerance?

>

Correct, they are not needed on the root domain DNS servers as the actual

zones can be located. However, if you envision those delegated DNS

servers being out-of-touch, then having a root domain DNS server local

copy would allow resolution of names in that delegated domain (but,

of course in that circumstance those hosts would likely not be reachable).

> -I noticed that I could add host records to the replicated \_msdcs zone

from

> the root zone from the sub-domains dns server. It there any issues with

> this? I just want to make sure that this is correct that they should be

able

> to add records.

>

All DCs need to maintain records in here. That does not mean that

you need to have all DCs enlisted in this DNS application partition

(that is, it does not have to be replicated to the DCs as an AD integrated

## microsoft.public.windows.server.dns: Re: Windows 2003 DNS Setup for Sub-Domain off of Root

and hence primary zone). If the child domain DCs are enlisted, then the admins there will have a primary, and equal, copy of the zone in their DNS server and hence under their shared management.

> -When I type the fqdn and ip address in the delegation wizard, do I just add

> or delete the entries if I ever move the dns server to another server. I am

> just wondering if there are any gottcha's about moving zones to another dns server when using delegated zones.

>

The delegation needs to name the DNS servers that hold the zone, at least those that you want to be discoverable using the delegation. That means you would have an NS record for all such DCs (whether they hold a primary or secondary copy of the zone).

> -I also have a question that pertains to my domain upgrade process. I plan

> on installing a new bdc into the domain. I will then promote it to the pdc.

> Windows 2003 setup will be ran and the server will have dcpromo ran. Since I

> will not keep the upgraded 2003 server, I would like to have DNS for the

> upgraded domain on a member server in this domain that will be upgraded to a

> permanent dc. The question that I am struggling with is what should the dns

> server setup on the member server be. When I test this setup in my test lab,

> dcpromo give me a ldap error.

>

If you are going to go about it that way you need to make sure the relevant zones are configured to allow unsecured updates for the duration of the time when this DNS server is a member. Make sure that the machines (DC being upgraded) are using this DNS server in their Tcp/Ip config.

As an alternative, if you have already established the root domain you can just use the DNS servers of the root domain throughout this process and then move the zones after the fact. This route can have some short burps during the subsequent transition, and these can be minimized if you first define a new primary AD integrated forward zone for the child on the root domain DNS - this way at promo of the child the records are separated out into a separate zone instead of becoming part of the root domain's zone.

> Thanks in advance for any information.

>

> Mike

>

>

> "Roger Abell" wrote:

>

> > The operative requirement in your case was stated at the end

> > > I would like to have a DNS zone on each of the sub-domains

> > > that will be administered by remote administrators.

> > This implies that you also do not want them to be able to

> > alter the DNS support of the other domains.

> > In this case, you will need to have the zone supporting their

> > domain configured so that their DNS server(s) is(are) primary

> > for their domain but not for the others.

> > This in turns means that the root doman will need to have

> > proper delegations for the subdomains to their server(s).

> > Next, this means you will not be able to use enlistment of

> > the DNS on the child domain DCs into the forestroot DNS

microsoft.public.windows.server.dns: Re: Windows 2003 DNS Setup for Sub-Domain off of Root

```
> > application partition, but instead will either need to have
> > these all forward to the DNS servers of the forest root, or
> > will need to place secondary copies of the forest root DNS
> > zone on these child DNS/DCs. Placement of secondary
> > copies of other child domain zones in the different child
> > domain DNS/DCs is optional as these could be located by
> > the delegations that will be available from the root zone.
> > Just what you do place there would be governed by the
> > connectivity between the domains (full-time or not), etc..
> >
> > --
> > Roger Abell
> > Microsoft MVP (Windows Security)
> > MCSE (W2k3,W2k,Nt4) MCDBA
> > "Mike Graves" <MikeGraves@discussions.microsoft.com> wrote in message
> > news:AB832612-AEA7-4391-A75D-F3E795FA401F@microsoft.com...
> > > All;
> > >
> > > I am working on a migration of several NT Domain into a 2003 AD
Forest. I
> > > am going to be migrating the current NT domain into subdomains of my
new
> > > Forest. The question that I have pertains to the proper procedures
for
> > > setting up DNS for the sub-domains. I currently have ADI DNS setup on
the
> > > root domain. I need to know that proper way to have dns setup on the
> > > subdomains.
> > >
> > > Example
> > > Root.net
> > > Sub1.Root.net
> > > Sub2.Root.net
> > >
> > > I would like to have a DNS zone on each of the sub-domains that will
be
> > > administered by remote administrators.
> > >
> > > Thanks in advance for any info.
> > >
> > >
> > >
> > >
> > >
> > >
> > >
```