

# Re: DNS Redesign Issue

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2006-08/msg00656.html>

---

- *From:* "Jorge Silva" <jorgesilva\_pt@xxxxxxxxxxxx>
  - *Date:* Mon, 21 Aug 2006 18:08:11 +0100
- 

Inline

After I create the new AD primary zone in the child domain, delegate authority, and create the static records, do I want to set the new child domain DNS server as primary for the domain controllers?

–If you are going to create a new AD Integrated Zone in each child domain, then Yes, make sure that each DNS DC points to itself under Nic Preferred DNS settings. Also make sure that each child domain can resolve the TLD domain and the \_msdcs.domain.tld at the Root domain. This can be done by several types of configuration, I already gave you what I think that would be the the best In My opinion.

What about all the AD created records in the company.com domain? Should I run netdiag /fix and restart the netlogon service to recreate the records?

you can do that or stop and start the netlogon service, you can run dcdiag /test:dns to check if dns is Ok.

(You had mentioned forwarders previously, but if the network connection fails there will be issues.)

There're many pp that like forwarding (myself incl.), however if the link drops, than you're not able to resolve anything at the root because you can't connect to the servers.

—

I hope that the information above helps you

Good Luck  
Jorge Silva  
MCSA

Re: DNS Redesign Issue

Systems Administrator

"Jason1320" <Jason1320@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
news:7ED67C50-4078-4405-BBDA-93B6DC347725@xxxxxxxxxxxxxxxxxxxx

I think I have my question answered in that I will have to manually create  
at  
least some of the records, not a problem. I just want to clear up one  
more  
thing before we close this thread.

Currently all domain controllers point back to the TLD for either their  
primary or secondary DNS. This is because the TLD DNS server is the only  
writable NDS server right now. After I create the new AD primary zone in  
the  
child domain, delegate authority, and create the static records, do I want  
to  
set the new child domain DNS server as primary for the domain controllers?  
What about all the AD created records in the company.com domain? Should I  
run netdiag /fix and restart the netlogon service to recreate the records?  
(You had mentioned forwarders previously, but if the network connection  
fails  
there will be issues.)

Thanks,

Jason

"Jason1320" wrote:

We have hundreds of records for non-Windows servers and appliances. Most  
of  
these are unable to create their own records. There are also MX records,  
aliases, and SRV records that will not be automatically recreated. I need  
to  
do this as seamlessly as possible and missing anyone of these records  
would  
cause an outage.

Thanks,

Jason

"Jorge Silva" wrote:

-Why you want to export the Zone? The records are  
automatically created  
as  
long as you allow Dynamic updates?

## Re: DNS Redesign Issue

–Using DNS console you can right–click the zone and export to a File, however with this exported file you can't create a zone.

–To export a Zone and import that Zone in another DNS Server you need to use Dnscmd.

–C:\Dnscmd ServerName /ZoneExport child.domain.com  
Filename.dns (this file will be automatically created in DNS folder under System32, the File must have a .dns EXTENSION, the other problem with this is that you might need to change some information on that file, like for example the SOA owner, and/or the NS records, then you copy that file to the other DNS server, you can start by creating a new Primary zone then you have the option to give the name of the file that contains)

<http://technet2.microsoft.com/WindowsServer/en/library/ed0e4eeb-34a5-420e-aa6a-961ae5>

Attention you can only export and import a zone if that zone will be equal in the other DNS server, although you can export information to ONLY PART (like a delegation) you can't use that exported file you can't create a zone.

\*Using the Dns console:

Right click the zone that you want to export and choose the option export list, save the file "Test01.txt".

(Open the file and check the format)

Re: DNS Redesign Issue

\*Using Dnscmd

```
Dnscmd ServerName /ZoneExport child.domain.com  
Test01.dns
```

(Open the file and check the format)

-Compare both...

Now the real question here is why do you want to do that???

There's no  
need

to have all this work, DNS can dynamically register this  
records if you

allow it to do so. If you're concern about some manual  
created records

you

can export the zone using any of the above commands, and  
then just

create a

script with Dnscmd to create them automatically.

```
Dnscmd [ServerName]  
/recordaddZoneNameNodeNameRRTypeRRData
```

Check:

<http://technet2.microsoft.com/WindowsServer/en/library/ed0e4eeb-34a5-420e-aa6a-961ae5>

--

I hope that the information above helps you

Good Luck

Jorge Silva

MCSA

Systems Administrator

"Jason McKee"

<JasonMcKee@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in  
message

<news:4E27292B-EAAF-4FB8-9514-3D2D1BA124ED@xxxxxxxxxxxxxxxxxxxx>

From another news group:

From your description, my understanding on  
this issue is that you

would

like to change the current DNS design and

create AD integrated zone

## Re: DNS Redesign Issue

for  
each subdomain.

Unfortunately there's no efficient way to extract the domain information for dallas.company.com from the company.com zone. However, if you are using DHCP, clients should be able to dynamically and automatically register/update records with the configured DNS server, and you don't need to manually re-input everything.

Considering the current situation, we suggest you follow the guideline below:

1. Delete the current dallas(.company.com) and other subdomains on DNS server in the root domain
2. On DNS server in the root domain, delegate dallas to DNS server in the child domain
3. Create a child zone dallas on the DNS server in the child domain
4. Configure all clients in the child domain to use DNS server in the child domain as Primary DNS server
5. Add the parent (root) DNS server as a forwarder on the child DNS server.

For more information, please refer to the following documents:

255248 How To Create a Child Domain in Active Directory and Delegate the DNS Namespace to the Child Domain  
<http://support.microsoft.com/kb/255248>

323418 How To Integrate DNS with an Existing DNS Infrastructure If Active

Re: DNS Redesign Issue

Directory Is Enabled in Windows Server  
2003

<http://support.microsoft.com/default.aspx?scid=kb:EN-US:323418>

How DNS Support for Active Directory  
Works

<http://technet2.microsoft.com/WindowsServer/en/library/9d62e91d-75c3-4a77-ae93-a8804e9ff2a11033.msp?mfr=true>

"Jason McKee" wrote:

This is great information  
and I understand all these  
concepts but I  
think  
you  
are missing the point of  
what I am trying to do. In  
my top level  
domain  
I  
have one primary zone for  
company.com. That zone  
contains 9 sub  
domains  
(dallas.company.com,  
detroit.company.com,  
la.company.com, etc.) I  
want  
to  
delegate these domains but  
first I need to get the  
information out  
of the  
tld  
zone and into the primary  
zones that will be created in  
the child  
domains.  
If it were possible I would  
want to "cut" the Dallas  
folder from the  
company.com domain and  
paste it as the root of the  
child primary  
domain.  
I  
want to do this for all 9 sub  
domains. However this is

Re: DNS Redesign Issue

not possible  
so I  
want to find the easiest way  
to do it without recreating  
all of the  
DNS  
records.

Thank you,  
Jason McKee  
MCSE/MCSA (Messaging)  
2003

"Jorge Silva" wrote:

Hi again  
Looks like  
you're out  
of sync so:  
I'm going to  
try to  
provide you  
a solution  
(but  
remember  
you can  
have  
different  
implanted  
solutions to  
achieve the  
same thing),  
if you  
disagree  
with  
something  
please let  
me know.

You've 1  
top Root  
Domain and  
several  
child  
domains.

You want to  
design a  
DNS

## Re: DNS Redesign Issue

infrastructure  
for all  
domains.

–Objectives  
are:  
availability  
of the name  
resolution  
for all  
domains in  
the  
forest,  
reduce  
administrative  
work  
configuring  
them,  
reduce the  
Replication  
traffic.

–Ok,  
assuming  
that you've  
all DNS  
servers in  
DCs (Why  
on DCs,  
because  
you  
can benefit  
in terms of  
security,  
you can  
integrate it  
with AD,  
provide  
you  
less admin  
work and  
you can use  
replication  
to replicate  
the zones  
for  
existent  
DNS server  
in your

## Re: DNS Redesign Issue

network):

–Generally  
the Root  
Domain is  
used only  
for  
administration;

I  
don't  
know if  
this is your  
case, but  
generally  
the top root  
domain has  
few  
information  
on  
it, and is  
rarely  
changed in  
terms of  
changes,  
let's begin:

1–Using  
Stub zones  
in the root  
or child  
domains  
isn't  
generally a  
good  
idea,  
why? Well  
Stub zones  
do not  
remove the  
requirement  
for  
delegations,  
Stub  
zone data  
doesn't  
transfer  
during zone  
transfers  
like  
delegation  
information

## Re: DNS Redesign Issue

does, so if  
the parent  
zone is  
transferred  
without  
delegation  
information,  
how will  
server find  
child  
zones?), So  
configuring  
Stub zones  
aren't an  
option here.

–In the Top  
Root  
Domain you  
make the  
domain.tld  
and  
\_msdcs.domain.tld  
AD  
Integrated.  
Because  
you only  
have  
Windows  
2003 in  
your forest  
make  
sure  
that  
you have  
your FFL at  
Windows  
2003, Why?  
– Because  
among  
other  
things  
you can  
benefit with  
replication  
(only  
changes are  
replicated).  
Next  
configure

## Re: DNS Redesign Issue

delegation,  
delegate  
each child  
domain to  
the correct  
server(s).  
Configure  
the  
replication  
scope of the  
Top Root  
Domain  
"domain.tld"and  
the  
"\_msdcs.domain.tld"  
available  
across the  
forest.  
Why? –  
Well First  
we  
have  
availability,  
even if the  
link is down  
the name  
resolution  
works  
because all  
servers have  
a copy of  
that zone,  
including  
other  
CHILD  
domains NS  
records,  
so the  
servers can  
resolve the  
other child  
domains  
even if the  
link  
with the  
Top Root is  
down,  
Second we  
have less  
Admin  
work,

## Re: DNS Redesign Issue

because the zones will be transferred without any additional configuration, Third the \_msdcs.domain.tld contain information about Global catalog and other domain/forest important records and they only exist in parent (root) DNS server (this zone contains information that IS ONLY AVAILABLE IN THE ROOT), so is always a good practice to replicate the root \_msdcs.domain.tld across the forest.

– So why not Primary Zone? – To much configuration to be done, is un-secure, you can't

## Re: DNS Redesign Issue

benefit of  
AD  
replication,  
to use it in  
child  
domains  
you  
would  
need to  
allow zone  
transfer  
each time  
that you add  
anew DNS  
server  
(which  
represents  
more admin  
work).

– So why  
not  
Secondary  
Zone? –  
Well to  
have a  
secondary  
zone you  
must  
have a  
Primary  
Zone then  
you must  
configure  
that primary  
zone to  
allow  
zone  
transfers  
(more  
admin work  
each time  
that you add  
anew DNS  
server)  
and  
BTW  
Primary  
Zones are  
not secure  
as AD

Re: DNS Redesign Issue

Integrated  
Zones, But  
Wait a  
minute.  
We  
can have  
AD  
Integrated  
Zone, and  
configure  
other DNS  
Servers  
with  
Secondary  
Zones.  
Sure, but  
you still  
need to  
allow Zone  
transfer  
each time  
that  
you  
Add a new  
DNS server  
(More  
Admin  
Work), so  
why not use  
Replication  
and  
leave  
all Admin  
work for  
Windows,  
and we  
never have  
to worry  
about  
configurations  
and stuff  
like that.

What About  
Internet  
Resolution?  
Well we  
have  
Forwarding  
for that,  
you

## Re: DNS Redesign Issue

can  
benefit of  
Forwarding  
to allow  
Internet  
resolution  
in each  
domain.

Top Root is  
done.

Time to  
Child  
Domains:

-Child  
Domains:  
well  
because we  
already  
have the  
domain.tld,  
\_msdcs.domain.tld  
and all  
forest  
delegations  
in the DNS  
server(s)  
across the  
forest, this  
means that  
the child  
domains  
can resolve  
all existent  
domains,  
GCs,  
Existent  
Sites  
configuration,  
etc. So now  
we only  
need to  
configure  
the  
child zone  
itself,  
nothing  
more. Make  
it AD

Re: DNS Redesign Issue

Integrated,  
configure  
the  
replication  
scope to All  
DCs in the  
DOMAIN,  
and you're  
up and  
running.

Related  
Links:

How to  
Create a  
Child  
Domain in  
Active  
Directory  
and  
Delegate  
the  
DNS  
Namespace  
to the Child  
Domain

<http://support.microsoft.com/kb/255248/>

Conditional  
Forwarding  
in Windows  
Server 2003

<http://support.microsoft.com/default.aspx?scid=kb:en-us:304491>

How to  
configure  
DNS for  
Internet  
access in  
Windows  
Server 2003

<http://support.microsoft.com/kb/323380/>

--

I hope that  
the

Re: DNS Redesign Issue

information  
above helps  
you

Good Luck  
Jorge Silva  
MCSA  
Systems  
Administrator

"Jason  
McKee"

<JasonMcKee@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in  
message

[news:2155B3C6-1B0F-4C60-8666-EF73F1018A65@xxxxxxxxxxxx](mailto:news:2155B3C6-1B0F-4C60-8666-EF73F1018A65@xxxxxxxxxxxx)

I  
agree.  
The  
question  
is  
how  
to  
get  
the  
domains  
for  
the  
child  
zones  
out  
of  
the  
single  
existing  
zone  
for  
company.com.  
You  
can't  
simply  
copy  
and  
paste  
it,  
and  
recreating  
all  
the

Re: DNS Redesign Issue

records  
would  
take  
hours.  
And  
I  
don't  
want  
the  
whole  
company.com  
domain  
replicated  
to  
all  
the  
child  
domains.

Thanks  
Jason  
McKee  
MCSE/MCSA  
(Messaging)  
2003