

Re: DNS Redesign Issue

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2006-08/msg00614.html>

- *From:* "Jorge Silva" <jorgesilva_pt@xxxxxxxxxxxx>
 - *Date:* Sun, 20 Aug 2006 01:47:03 +0100
-

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 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 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 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 delegation, delegate each child domain to the correct server(s). Configure

Re: DNS Redesign Issue

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, 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 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 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 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 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

Re: DNS Redesign Issue

Re: DNS Redesign Issue

<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 information above helps you

Good Luck
Jorge Silva
MCSA
Systems Administrator

"Jason McKee" <JasonMcKee@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:2155B3C6-1B0F-4C60-8666-EF73F1018A65@xxxxxxxxxxxxxxxxxxxx>

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 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

"Jorge Silva" wrote:

As I already told you there are many possible configurations, for this to work, the most common is to delegate the child zones on tld to each child domain.

In each child domain you can choose by different type of possible configurations:

-If you configure Forwarding ("All other Domains" option - pointing to tld)
all queries will go to tld DNS server (including Internet resolution queries), if the link with tld is down then queries will fail for domains but the DNS server will attempt to use its root hints to resolve the queries
(unless you select the option don't use recursion for this domain).

-If you configure Conditional Forwarding, you can have better control where queries will go, and if the link is down for any particular domain, that doesn't mean that other queries will fail as long as you have a link up with

Re: DNS Redesign Issue

these domains.

–For secondary and stub zones: the big advantage of stub zones is that they'll refresh automatically the NS records for that domain, and you don't need to allow zone transfer for stub zones to work, but all queries will be sent to NS for these domains. As for Secondary Zones all queries can be resolved locally, but you need to allow zone transfer on each zone.

–For Active Directory Integrated Zones (require that the DNS is also a DC), you can always choose by replicate them across the domain or forest. This can have a significant impact on your replication traffic.

--

I hope that the information above helps you

Good Luck
Jorge Silva
MCSA
Systems Administrator

"Jason McKee" <Jason McKee@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:5E05FC44-4C9E-4801-B5E9-7FB6F58E18DC@xxxxxxxxxxxxxxxxxxxx

The stub zone idea would work but it is not ideal for my situation. If I create stub zones for each domain then I have no fault tolerance in the case that a link between the sites goes down.

Your other idea wasn't clear but I think you are suggesting that I intergrate company.com in to the AD and replicate it across the forest. I have thought of this as well and plan to use it as a worst case senario. Ideally what I want to do though is extract the DNS information for city.company.com from the company.com zone and import it in to a new city.company.com zone.

This is a tough problem and I appreciate all the help!

Thank you,

Re: DNS Redesign Issue

Jason

"Jorge Silva" wrote:

the dallas.company.com is a child domain
right?
you can in newly created ad intergrated zone
pointing to the tld or
create a
stubzone on the domain and replicate it
accross that new domain.

--

I hope that the information above helps you

Good Luck
Jorge Silva
MCSA
Systems Administrator

"Jason1320"

<Jason1320@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message

news:53042AA6-8A57-41CC-BAA6-FDE8E5C184F1@xxxxxxxxxxxxxxxxxxxx

I plan to use stub zones in
the top level domains. The
issue I am
having
is
getting the dns data from
dallas.company.com in the
tld domain to
the
newly
created ad intergrated zone.
I would like to do this
without
manually
recreating each record.

Thanks,

Jason

"Jorge Silva" wrote:

Re: DNS Redesign Issue

Hi

Currently
we
have
one
root
domain
in
a
single
AD
forest.
Under
that
root
we
have
9
child
domains,
all
one
layer
below
the
root.
All
DC's
are
2003.

Hoooo my
GOD so
many
domains,
did you had
any especial
reason to
make
10
domains?

What
I
would
like
to

Re: DNS Redesign Issue

do
is
create
AD
integrated
zones
for
each
domain
and
delegate
authority
from
the
primary
zone,
company.com.
The
problem
that
I
am
running
in
to
is
how
to
get
the
data
from
the
subdomains
out
of
the
primary
zone,
company.com,
and
in
to
the
newly
created
AD
intergrated
zone.
I
only

Re: DNS Redesign Issue

want
the
information
that
is
critical
to
each
domain.
(i.e.
for
dallas.company.com
I
only
want
the
information
below
the
dallas
folder
in
company.com.)

Basically
you need to
create a tld
DNS
domain
make it AD
Integrated,
and
delegate the
child zone
to the other
DCs in sub
domains, by
delegating
the
zones the
tld domain
knows
where to
find the NS
for these
domains,
the
problem
should
come how

Re: DNS Redesign Issue

the child
domains
resolve the
tld domain,
and
there
several
methods for
this, but
you're
replicating
the tld to
the
child
domains so
you need
not to
worried
about that.

Check:

Best
practices for
DNS client
settings in
Windows
2000 Server
and
in
Windows
Server 2003

<http://support.microsoft.com/default.aspx?scid=kb:en-us:825036&sd>

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

<http://support.microsoft.com/default.aspx?scid=kb:en-us:255248&sd>

--

I hope that
the

Re: DNS Redesign Issue

information
above helps
you

Good Luck
Jorge Silva
MCSA
Systems
Administrator

"Jason1320"

<Jason1320@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in
message

news:1697112D-E13F-4066-9500-0DCAC8F2A028@xxxxxxxxxxx

I
am
trying
to
redesign
DNS
for
a
company
I
just
joinedbut
I
have
come
across
an
issue
that
I'm
not
sure
how
to
get
around.

Currently
we
have
one
root
domain
in
a

Re: DNS Redesign Issue

single
AD
forest.
Under
that
root
we
have
9
child
domains,
all
one
layer
below
the
root.
All
DC's
are
2003.

DNS
is
setup
as
follows.
The
root
domain
contains
one
DNS
server
with
a
single
primary
zone
of
company.com.
Each
child
domain
has
a
secondary
"copy"
of
this
zone

Re: DNS Redesign Issue

on
at
least
one
server
in
the
domain.
Within
the
primary
zone
there
are
folders
for
each
domains
subdomain.
(Example:
dallas.company.com)
Each
domain
controller
is
configured
to
write
back
to
the
primary
zone
to
make
updates.

What
I
would
like
to
do
is
create
AD
intergrated
zones
for
each
domain

Re: DNS Redesign Issue

and
delegate
authority
from
the
primary
zone,
company.com.
The
problem
that
I
am
running
in
to
is
how
to
get
the
data
from
the
subdomains
out
of
the
primary
zone,
company.com,
and
in
to
the
newly
created
AD
intergrated
zone.
I
only
want
the
information
that
is
critical
to
each
domain.

Re: DNS Redesign Issue

(i.e.
for
dallas.company.com
I
only
want
the
information
below
the
dallas
folder
in
company.com.)

Any
suggestions?

Thank
you,

Jason