

Re: Replication issues

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-09/msg01305

- *From:* George <George@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 20 Sep 2006 06:50:02 -0700
-

Sorry Herb,

I wanted to say Zone Transfers not Zone Forwarding. Long day yesterday.

Yes, I have set up the Conditional Forwarding for internal .local domains and left the ISP forwarders for All other domains. I had this configured only on 2 servers out of 4 DNS servers. Thanks for your help. I read this great article also that explains recursive and iterative queries, difference of 2000 DNS and 2003 DNS and how to set up Conditional Forwarding.

Cheers

Conditional Forwarding in 2003

http://www.window networking.com/articles_tutorials/DNS_Conditional_Forwarding_in_Windows_Server_2003.htm

"Herb Martin" wrote:

"George" <George@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:9A37D80E-6116-48CA-9CA1-8438AD39BBC9@xxxxxxxxxxxxxxxxxxxxx

Thanks Herb. For starters, I checked all of the DCs which are DNS servers. It turned out that some didn't have forwarders on the server level to ISP servers not to mention servers in the other domains. So for experimenting purposes, I have populated the forwarders on all DNS servers to ISP servers and then to other domain and vice versa.

You cannot reliably use UNCONDITIONAL forwarding to get different sets of answers -- just as a client cannot use both internal and external DNS servers on the NIC->IP properties.

IF you use unconditional forwarding to the ISP you MUST use conditional forwarding (or another method) reach those specific internal domains within your network -- otherwise your DNS server will (randomly and unpredictably) bypass

Re: Replication issues

the internal servers whenever it happens to use the ISP.

This now enabled me to do nslookup on each server from each server by using server dnserver1.abc.local and so on to check each dns if it can resolve other ones. It took couple of minutes but after forwarders were added, I was able to resolve all of the hosts from each domain and vice versa using all of my dns servers by using server command to change the server that is being used for resolution. This was not the case before the change.

Sounds like you might have gotten it right.

I left zone forwarding unchecked as I dont have primary and secondary DNS server. I believe we would use this if not in 2003 and not AD integrated zone is the type. Corect or I missundestud what you wrote?

There is no such thing as "zone forwarding" but I can imagine that someone might use that term for "Conditional Forwarding" so if that is what you mean you have to reread my paragraph above and either NOT forward at all to the ISP from those DNS servers which use UNCONDITIONAL FORWARDING internally, (and that may still be tricky to get right) OR you must use Conditionally Forwarding for all "sister" DNS hierarchies internally AND ONLY use Unconditional Forwarding to the ISP.

So far no errors in event viewer. thanks for your help again. I am good now. Cheers.

If you have that mix which I advised against above you may not see the problem right away but it will never be reliable nor is it setup correctly.

--
Herb Martin, MCSE, MVP
Accelerated MCSE
<http://www.LearnQuick.Com>
[phone number on web site]

"Herb Martin" wrote:

"George" <George@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote
in message

Re: Replication issues

news:0F85EC5E-782A-443C-A8F9-54CAAFE06EF4@xxxxxxxxxxxxxxxxxxxx

Herb,

Thanks for your help. This does make sense.
I do have 2 diferent sets
of DNS
as one is for abc and other for def domain.
Servers have forwarders (to
ISP
DNS) but zones have no Zone Forwarding
enabled. Could that be a part of
the
issue?

Zones don't do individually forwarding; only servers
FORWARD,
either Generally (for all other names) or (Win2003 only)
Conditionally
Forward to specific server sets for specific DNS trees (i.e.,
forwarding
to the DNS servers at the top of a DNS hierarchy essentially
forwards
for all names BELOW that parent DNS server set.)

In your specific case, the natural step would be for servers
holding
DEF to CONDITIONALLY forward to ABC servers, and
vice versa.

There are additional choices but this is one good choice. [My
favorite
is usually to just have every DNS server in the Win2003
Forest run
on the DCs and then use AD Integrated DNS with
Forest-Wide Replication.]

I am also confused if zone transfers are
needed and which one to
enable.

Zone transfers are needed (and generally automatic) TO
YOUR
SECONDARIES, usually from the Primary, but technically
from
any DNS server holding that SAME ZONE.

Most such confusion emanates from thinking about "more

Re: Replication issues

than
one zone at a time". You should form the STRONG habit of
thinking of one DNS zone at a time. Zones are unrelated to
each
other, with the very limited exception of when a Parent zone
delegates to the DNS servers of a Child zone.

Figure out DNS one zone at a time. Make sure that each
DNS
server can find all of the names it's clients will EVER need,
whether it holds those names in a local zone, conditionally
forwards to other specific DNS servers which hold the
needed
names, OR recurses from the root down itself or
unconditionally
forwards to a DNS server which can find other names by
doing
one of the above.

I have _msdcs.abc.local and abc.local which
are both AD integrated.
abc is ad integrated but is only for abc
domain servers and def is also
the
same. _msdc.abc.local is ad integrated and it
is for all the servers in
the
forest abc.local.

Then this latter _msdcs should appear on EVERY DNS-DC
in the
forest unless they are running Win2000 which doesn't
support forest
wide replication of DNS in AD.

I will be doing more testing but it seems
DNS issue at the
moment; you are right. So, what should I do
to start isolating the
issue? In
which order rather and what to look for.
Thanks in advance,

Better to understand the issues (above) and then work it out
logically (with our help). No "cookbook" method will protect
you from all possible errors nor help you solve any specific
error most rapidly.

Re: Replication issues

Treat each zone as separate. Stop thinking of a DNS server as being "solely for a particular zone" since it can hold many zones and must find EVERY zone or name the clients which use it will ever need.

We all make the latter mistake to SOME extent, if for no other reason than it is a convenient way of speaking. That is, the server which holds the "xyz.domain" SEEMS easier to name as the "xyz-DNS server" but really it must find EVERY name that it's (presumably xyz) clients will EVER legitimately need.

Each DNS server must find all of these names whether it holds the zone physically, knows the server which does, recurses from the root (or the Internet) down, or forwards to another server which does so.

DCDiag is a great tool which should be run on every DC regularly AND any time you suspect a DNS or AD/Replication issue.

NSlookup is how you ask a direct question to determine if a name can be resolved, or (even better) ask a SPECIFIC DNS server to do that resolution to see if one DNS server may work while others do not:

```
nslookup name.tocheck.domain  
Optional.IP.DNSServer.ToAsk
```

This latter form is used far too infrequently by people who don't really understand how CLIENT DNS resolution and DNS Server DNS resolution are two different but complementary parts of the mechanism.

"IPConfig /all" is also your friend, mainly to ensure that no DNS

Re: Replication issues

client has any "external DNS" server set in NIC->IP properties that would bypass internal DNS servers, and thus miss resolving all internal names.

Below are my general recommendations on DNS for AD:

- 1) Dynamic for the zone supporting AD
- 2) All internal DNS clients NIC\IP properties must specify SOLELY that internal, dynamic DNS server (set.)
- 3) DCs and even DNS servers are DNS clients too -- see #2
- 4) If you have more than one Domain, every DNS server must be able to resolve ALL domains (either directly or indirectly)

netdiag /fix

...or maybe:

dcdiag /fix

(Win2003 can do this from Support tools):
nltest /dsregdns /server:DC-ServerNameGoesHere
<http://support.microsoft.com/kb/q260371/>

Ensure that DNS zones/domains are fully replicated to all DNS servers for that (internal) zone/domain.

Also useful may be running DCdiag on each DC, sending the output to a text file, and searching for FAIL, ERROR, WARN.

Single Label domain zone names are a problem Google:
["SINGLE LABEL" domain names DNS 2000 | 2003 microsoft:]

--

Herb Martin, MCSE, MVP
Accelerated MCSE
<http://www.LearnQuick.Com>
[phone number on web site]

"Herb Martin" wrote:

Re: Replication issues

"George"

<George@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in message

news:73032244-FE21-4C6D-99A5-600E0C0F9F6A@xxxxxxxxxxxxxxxxxxxx

Hello all!

Got couple
of problems
and some
strange
DNS
resolution
happening
and
can
not
find the
cause or
resolution
of/for the
issue.
Anyways,
we are 1
forest, 2
domains.
Domains
are
abc.local
and
def.local.

How do DNS servers in abc
resolve def and vice versa?
(e.g., Hold the other zone,
use conditional
forwarding?)

abc is in
Chicago
and Reno
and
def is in
Shanghai.
Users and
admins in
def.local
have no
administrative

Re: Replication issues

permissions
to abc while
abc has all
permissions
to def. def is
not
in
enterprise
group.

None of the above much
matters to DNS or general
authentication.

All 3 sites
are
connected
via VPN
tunnels
(CISCO
PIX) and
DNS is AD
integrated
with Secure
selected for
update. I am
seeing
event id
1925, 1926,
1865, 1311
and 1566 in
Reno server
but nowhere
else.
This
server
is resolving
servers in
def.local as
server1.abc.local
instead of
server1.def.local
for what
ever reason
and I can't
figure out
why.

Re: Replication issues

No it is not. DNS servers
ONLY resolve the precise
names
that they contain or can
reach on other DNS servers.

If someone on a def.local
domain CLIENT types
merely "server1"
then their WORKSTATION
resolver will append their
own DNS
suffix and thus resolve
server1.def.local IF it exists.

That is, such is a CLIENT
side effect due to default
suffix addition.

Other
servers are
resolving
ok. I am
doing
simple ping
to server1 in
def.local
from
Reno with
out
specifying
the domain
prefix

Do you mean SUFFIX?

You client machine will
append it's own suffix, and
perhaps parent
suffixes and any custom
suffixes you added.

Ping is NOT the best choice
for troubleshooting a
problem once
you determine (or strongly
suspect) a DNS problem.

Re: Replication issues

Use NSLookup, with full domain names, and even supply the specific DNS server to test each separate:

```
nslookup name.domain.com  
IP.DNS.Each.Server
```

Do you by any chance have BOTH DNS servers defined on the clients but no way for the two SETS of DNS servers to reach the other set?

and it is
resolving it
again as
server1.abc.local
instead of
server1.def.local.
Strange.
Anyone has
any
ideas.
Please ask
questions as
I could have
missed
some
important
details.

DNS CLIENTS must be set to use ONLY the DNS server set which can resolve EVERY NAME they will (ever legitimately) need.

When you have two separate DNS server sets then each set must have some way to find the 'other' set if clients are to find those names.

Re: Replication issues

Readmin
/showism
shows good
results. I
have no
bridgehead
servers
defaulting

One would hope you do
have bridgeheads servers
(being chosen
by the KCC usually) since
replication will not work
across Sites
without this.

[Unless you have such a
WAN with no sites which is
a poor idea
in almost all cases. Cross
domain bridgehead may not
show in the
Sites and services however
even though technically
some info is
replicated across Domains.]

Usually the best way to
check DCs and DNS
quickly is to use
DCDiag on each DC.

and use
KCC to
figure out
the
replication.
IP is being
used and
there is
only
one site link
and all 3
sites are
members.
Please help.

Re: Replication issues

Although many people don't realize that one SiteLink for three (or more) Sites is legal it may make perfect sense: Essentially it means that you are declaring all Sites to replicate with each