

Re: Active Directory Integration in DNS – Looses Forward Zone :-0

Source:

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.dns/2006-04/msg00086.html>

- *From:* "Marvin Miller" <sales@xxxxxxxx>
 - *Date:* Sat, 15 Apr 2006 22:23:43 -0700
-

Hi Kurt;

Thanks for replying :-)

"did you transfer the 5 Flexible Single Master Operations (FSMO) roles the the second DC? "

I doubt it as I don't know what those are. All I did was run DCPROMO on the DC and ensure that the new DC was a catalog server. I followed a MS KB article and it seemed to work fine. The previous DC is now a normal server although for some reason it seems to still run the File Replication Service.....

"I'm not sure why you can't create a DNS zone for your domain name, but if you haven't transferred the FSMO roles, do that first and try again."

Can that still be done after the original DC has become a normal server? If so, how do I do that?

Thanks very much;
Marvin

"Kurt" <lorentzenkurt@xxxxxxxxxxxxxxxxxxxx> wrote in message
<news:1243fmv9qgj5e15@xxxxxxxxxxxxxxxxxxxxxxxx>

Several things here. When you demoted your first DC (there are no PDCs and BDCs anymore), did you transfer the 5 Flexible Single Master Operations (FSMO) roles the the second DC? Only AD Integrated DNS zones can accept dynamic updates. Don't confuse dynamic updates with incremental zone transfers. Dynamic updates are just hosts registering themselves in DNS so you don't have to add the records manually. Since you now only have one

DC,

Re: Active Directory Integration in DNS – Loses Forward Zone :-0

you won't have any AD replication, and therefore no incremental zone updates. I'm not sure why you can't create a DNS zone for your domain

name,

but if you haven't transferred the FSMO roles, do that first and try

again.

You'll actually have to seize the roles rather than transfer since you already demoted your first DC (which likely held all 5 roles).

...kurt

"Marvin Miller" <sales@xxxxxxx> wrote in message
news:O%23L2adNYGHA.3448@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi Folks;

I have a problem with DNS that's stemming from Active Directory integration

(as near as I can tell).

First, I know next to nothing about AD – I'm still coming from the realm of

NT 3.5/4.0 and PDC's and BDC's. My network is small so AD is just something

I need installed and working. Here's what's happened.....

All machines are Windows 2000 and I had an AD PDC that worked just fine. There was also an AD BDC machine. Network changes caused me to need to remove AD from the PDC and promote the BDC to a PDC and run with one

PDC.

To that end I ran DCPROMO on the machine that I no longer wanted to be

and

AD server. I made sure beforehand that the BDC was also a catalog

server.

Everything went well, the BDC became a PDC and authentications worked

etc.

I then changed the new PDC so that it would not be compatible with pre-Windows 2000 domains. This is not necessary for me so I thought that

Re: Active Directory Integration in DNS – Loses Forward Zone :-0

Re: Active Directory Integration in DNS – Looses Forward Zone :-0

was
a good thing to do.

The new PDC is also the primary DNS server set to allow dynamic updates. When the changeover occurred everything was fine. When I later re-booted the new PDC I found that the DNS had lost the forward zone for my domain!

Also

an event viewer entry was logged;

Event ID 5773;

The DNS Server for this DC does not support dynamic DNS. Add the DNS records from the file '%SystemRoot%\System32\Config\netlogon.dns' to the DNS server servicing the domain referenced in that file.

I found the file but have no idea as to how to get it 'into' the DNS server.

I tried copying the file to the DNS server directory and re-starting the service but that didn't work. I then tried un-installing DNS, re-installing

it and making a new Active Directory Integrated forward zone. That will work – but only if I choose a zone name that is different than the previous existing one. If I try to choose the existing zone name I get an error message stating;

The Zone cannot be created.
The Zone type is invalid.

It's as if the registry contains information on that zone and won't

allow

me to create it. I then thought to myself, "Do I have to have an AD integrated DNS?" – remember, I know little about this. So I then made a new

standard

zone and it worked fine. The problem is that I get entries in the event viewer saying to the effect that Active Directory is trying to do

dynamic

Re: Active Directory Integration in DNS – Loses Forward Zone :-0

updates to the DNS but it's not working – with multiple Stop Signs each time

AD tries to add an entry :-0

As a workaround, I made my Primary DNS server a secondary, made my secondary

a primary and then did a zone transfer from it! (because the secondary

DNS

server still had the AD integrated information for the forward zone).

This

worked and I then promoted the AD DNS back to primary and demoted the other

DNS server back to a secondary. I ensured that the AD integrated Primary DNS

server was set to allow dynamic updates and all is perfect. Until I re-boot the machine.

Once I reboot the AD machine it drops the entire forward zone and then logs

the same error;

Event ID 5773;

The DNS Server for this DC does not support dynamic DNS. Add the DNS records

from the file '%SystemRoot%\System32\Config\netlogon.dns' to the DNS server

servicing the domain referenced in that file

The forward lookup zone on the AD DNS server is set to allow Dynamic Updates. It's also set to load Zone Data on Startup from Active

Directory

and Registry.

I'm pretty sure I'm missing something simple here and that it's caused

by

my

lack of basic AD understanding. Can anyone tell me what needs to be done to

fix this issue?

Thanks VERY much !

Re: Active Directory Integration in DNS – Loses Forward Zone :-0

Re: Active Directory Integration in DNS – Looses Forward Zone :-0

Marvin Miller