

Re: Automatic primary zone to primary zone transfers???

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2005-12/msg00156.html>

- *From:* "Herb Martin" <news@xxxxxxxxxxxxxxxx>
 - *Date:* Fri, 9 Dec 2005 01:50:39 -0800
-

"Joe Flowers" <flowers@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:ujgYkx%23%23FHA.228@xxxxxxxxxxxxxxxxxxxxxxxx

> Thanks a lot Herb! This was very helpful.

>

> Something wierd though:

> I turned the built-in MS ICS firewall on the servers and AD started back

> to replicating correctly. Ouch!

[That is the ICF (firewall) even though ICF and ICS are on the same dialog.]

That is extremely weird. It should be the other way around.

(I assume you have a typo above.)

If you turned it OFF it SHOULD replicate but it SHOULD FAIL
if the ICF is on in many case.

Notice it might not fail always since this DC might be the initiator
of the replication, but it will fail FROM any DC with the ICF
(or BASIC RRAS) firewall running.

> I thought that ICS would have recognized that it was running on a DC and
> automatically opened the correct ports/etc. for correct AD sync.

Why? ICS isn't even built particularly for a server.

Even BASIC Firewall (in RRAS) which is similar wouldn't
do that.

> Any ideas on how I can re-enable ICS AND have AD replicate correctly?

No, not really. You could define all needed ports but that
would open it to ALL client addresses which would largely
invalidate the reason for a 'firewall'.

Use IPSec instead, even though you will never enable the
actual IPSec protocols. Use IPSec to build a PASS and BLOCK
filter only.

Re: Automatic primary zone to primary zone transfers???

Notice that it makes little sense to turn on a firewall like ICS for a DC — ICS is all or nothing except for Port definitions, and even then it is for ALL clients.

Most people don't realize that IPSec policies can be used for simple (and complex) BLOCK/PASS filters with no actual IPSec ever invoked.

--

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

>
> Joe
>
>
>
> Herb Martin wrote:
>> "Joe Flowers" <flowers@xxxxxxxxxxxxxxxxxxxx> wrote in message
>> news:%232qdzJo%23FHA.1676@xxxxxxxxxxxxxxxxxxxxxxxx
>>
>>>Hmmm... They are AD Integrated DNS servers. There must be something else
>>>wrong then? Let me check the AD replication status.
>>>
>>>Thanks Herb. Thanks a lot!
>>>
>>>I'll see what DCdiag tells me.
>>>
>>>Does anyone else have any ideas please?
>>>
>>
>>
>>
>> Well, in that case it is likely a DNS problem that is
>> causing a failure of AD replication (check DCdiag)
>> and therefore the replication of DNS itself (because
>> DNS is AD Integrated.)
>>
>> You might want to point EVERY DC (on the NIC IP
>> DNS Settings) to the "best" DNS server — get the all
>> registered — get AD replicated. Then you can point
>> them back to themselves.
>>
>> Here are the general settings 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.)

Re: Automatic primary zone to primary zone transfers???

Re: Automatic primary zone to primary zone transfers???

>> 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:]
>>

• References:

- ◆ [Automatic primary zone to primary zone transfers???](#)
 ◇ From: Joe Flowers
 - ◆ [Re: Automatic primary zone to primary zone transfers???](#)
 ◇ From: Herb Martin
 - ◆ [Re: Automatic primary zone to primary zone transfers???](#)
 ◇ From: Joe Flowers
 - ◆ [Re: Automatic primary zone to primary zone transfers???](#)
 ◇ From: Herb Martin
 - ◆ [Re: Automatic primary zone to primary zone transfers???](#)
 ◇ From: Joe Flowers
-
- Prev by Date: [How to configure DNS for forest trust](#)
 - Next by Date: [Re: How to configure DNS for forest trust](#)
 - Previous by thread: [Re: Automatic primary zone to primary zone transfers???](#)
 - Next by thread: [Re: How to export all dhcp records in text/csv file](#)
 - Index(es):
 - ◆ [Date](#)
 - ◆ [Thread](#)