

Re: Secondary Zones All Stopped Working – Win2003

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2004-09/0169.html>

From: Andrew Hodgson (*me3_at_privacy.net*)

Date: 09/04/04

Date: Sat, 04 Sep 2004 19:11:47 +0100

On 4 Sep 2004 09:46:43 -0700, tomrossi7@gmail.com (Tom Rossi) wrote:

>Andrew Hodgson <me3@privacy.net> wrote in message
news:<06shj050cm990mkms44g431tm7aupqs9@4ax.com>...
>> On 2 Sep 2004 05:38:45 -0700, tomrossi7@gmail.com (Tom Rossi) wrote:
>>
>> >Andrew Hodgson <me3@privacy.net> wrote in message
news:<vk4cj0ld5bcn7e818go2fbgfku5m4ccnf@4ax.com>...
>> >> On 30 Aug 2004 11:36:21 -0700, tomrossi7@gmail.com (Tom Rossi) wrote:

[...]

>> >> *Just a side note, are those public facing DNS servers for the
>> >> Internet? If so, is the secondary trying maybe to get the data from
>> >> the public IP of the primary nameserver and failing (this would
>> >> usually fail after the expire value in the SOA record had exceeded).
>> >> In any case, if they are public facing servers, they should really be
>> >> in two different locations, as you have no fault tolerance.
>> >>
>> >The primary server is a "public facing" DNS server for use by the
>> >Internet. The secondary server is an internal use only private DNS.
>>
>> Don't do that. The two DNS servers need to have separate zones, one
>> for the public (Internet facing) zone, and the internal one contains
>> internal data, including AD records, and internal/private DNS data.
>> Secondary servers are also needed for your public facing DNS server,
>> and it is best to either host these yourself at quite different sites,
>> or get a comercial outfit to host the secondary DNS for you
>> (relatively cheap). If you have internal data and want a secondary
>> for that, get a second domain controler. Do not make the secondary
>> for your internal server the external server, because then people
>> would be able to gleam data on your set-up by querying the external
>> server, and if the internal/external domain is the same, it can really
>> screw things up by giving out private DNS data in its results.
>>
>> Andrew.*

>

>Andrew,

>

>Thanks for the reply. The zones we are talking about have very few
>records: a webserver and a mailserver. I understand what you are
>saying, but I don't think that has a bearing on the issue I ran into.

It does if Internet users can't send you mail because your primary is
down. If you could let us know the domains (only one would be enough)
that had this issue, I may be able to help, as it is, now, though, I
am stabbing in the dark because I am not sure what you have done.

>My concern is that 2003 DNS may not be a good solution for someone
>like me that is hosting more than 50 zones with very few records.
>2000 worked flawlessly, but 2003 appears to have issues.

Going on your message, I am still convinced that your problem is the
way you have implemented it, and not the software itself.

Andrew.

--

Andrew Hodgson in Bromyard, Herefordshire, UK.
My Email: use <andrew at hodgsonfamily dot org>.