

Re: DNS and RRAS (revisited)

Source: <http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.dns/2004-11/0650.html>

From: Kevin D. Goodknecht Sr. [MVP] (*admin_at_nospam.WFTX.US*)

Date: 11/30/04

Date: Mon, 29 Nov 2004 19:10:11 -0600

In news:1c4b3f48.0411291616.147c9c19@posting.google.com,
DublStuf <Alan@caseware.com> commented

Then Kevin replied below:

- > *"Kevin D. Goodknecht Sr. [MVP]" <admin@nospam.WFTX.US>*
- > *wrote in message*
- > *news:<uI2q2Kk1EHA.3448@TK2MSFTNGP09.phx.gbl>...*
- >>
- >> *So your internal domain is domain.local?*
- >> *You can create entries in the system's hosts file for*
- >> *the internal server's names to fix this. What happens is*
- >> *without the hosts file entries the queries go out and if*
- >> *the hotel's DNS answers with not found before your*
- >> *internal DNS server can respond the query fails and the*
- >> *negative answer is cached, causing your issue. By adding*
- >> *the entries to the hosts file, these entries are loaded*
- >> *into the DNSCache and would go to any DNS servers,*
- >> *resolving the issue.*
- >>
- >
- > *Yes, we're using "domian.local" for our internal*
- > *namespace. Hosts*
- > *files would (and do) work for the name resolution*
- > *problem, which is*
- > *originally what I wanted to do-- run a script to query*
- > *the internal*
- > *dns and create a hosts file and distribute it to remote*
- > *clients via a*
- > *GPO with slow link detection turned off... or something*
- > *along those*
- > *lines. But I've been "told" that hosts files are not a*
- > *satisfactory*
- > *resolution to the problem (by management). :(*

Hosts file may be your only option to work around this. (read on)

- > *The problem that was happening with the hotel was that*
- > *their DNS*
- > *server would give a *positive* answer to*

microsoft.public.win2000.dns: Re: DNS and RRAS (revisited)

- > *"anyhost.domain.local" that*
- > *it had no business giving, of something like 10.0.0.1*
- > *(the gateway IP*
- > *on the hotel network). Whereas all hosts on our internal*
- > *"domain.local" network are in the 192.168.xx.xx range.*

Another example of why admins should stay clear of wildcard records.(read on)

- > *I've set up a test environment with conflicting DNS*
- > *information for*
- > *the same zones where I can duplicate the behaviour (using*
- > *a seperate*
- > *remote primary DNS server for "domain.local" with*
- > *conflicting records,*
- > *placed on the same subnet as the vpn client).*

I will give you another interesting option I have used one time before that works great, see below.

- >
- > *So what would happen is that the name would get resolved*
- > *first by the*
- > *DNS server on the foreign network by the "Local Area*
- > *Connection" to an*
- > *incorrect IP (the hotel's gateway) and no other DNS*
- > *servers (like the*
- > *ones from the PPP adapter) would be tried. I found an*
- > *interesting*
- > *article on the order which XP queries DNS servers from*
- > *each of its*
- > *interfaces:*

> <http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/docume>

- >
- > *Basically this article says that the 'preferred'*
- > *adapter's first DNS*
- > *server will be queried first and if it gets an immediate*
- > *answer,*
- > *that's what it goes with. So I'd like to find a way to*
- > *make the*
- > *remote connection adapter the 'preferred' adapter when a*
- > *remote*
- > *connection is active. Any ideas? Binding order didn't*
- > *seem to have*
- > *any effect on it...*
- >
- > *Another potential solution is to have them run "netsh"*
- > *scripts upon*
- > *vpn'ing and again after disconnection, to alter the DNS*
- > *setting on the*

- > *Local Area Connection to our servers and then back to*
- > *DHCP. But these*
- > *are execs and they don't want to be bothered with running*
- > *extra*
- > *scripts either, apparently we need to "make it work" so*
- > *it's*
- > *completely transparent to them. I guess I should check*
- > *if there are*
- > *'connect' and 'disconnect' scripts that can be set on the*
- > *2003 VPN*
- > *server... somehow I think 'disconnect' will be tricky*
- > *though, and may*
- > *be prone to leaving their adapter with internal DNS*
- > *settings, at which*
- > *point they would be unable to resolve names on the*
- > *Internet.*

I understand what you're going through and I feel your pain. Many admins recommend using the .local Top Level Domain for internal domain names, I usually recommend against it because it causes the exact problems you're having. This is why I recommend using a third level of the public domain name, as does Microsoft, so that you can delegate the internal name in the public zone, this is the exact setup I have.

But you're not using the third level name and you're using the .local TLD you will have to use hosts files.

I have used one other resolution in a case like you have that has worked but requires a regular connection to the internal network. When I say regular that means depending on the Expire time on the SOA record as to how often you must connect.

I installed BIND DNS on a XP laptop, then pulled a secondary zone from the AD DNS server for the .local AD zone because this particular user didn't want to have to keep updating a hosts file. I did increase the expire time on the zone to 28 days for this domain so the laptop can actually go for 28 days before the zone expires, but I could have settled for a week or so since he usually connects at least once a day. The BIND DNS does not have a forwarder configured it just uses Root Hints for external resolution. It would require that the VPN connection have a reserved IP address so that you can allow zone transfers to the laptop when it connects. Since the BIND has a secondary zone it will try to contact the Primary to check for a newer zone using the refresh and retry values to check the primary. So until it is connected to the VPN it cannot retrieve its new zone, once connect it usually only takes a few minutes.

It is either this or the hosts file. There is a benefit to using the BIND resolution, you have connectivity to a DNS server 100% of the time regardless of whether you are connected to the internet or not.

--
Best regards,
Kevin D4 Dad Goodknecht Sr. [MVP]
Hope This Helps
=====

microsoft.public.win2000.dns: Re: DNS and RRAS (revisited)

When responding to posts, please "Reply to Group" via your newsreader so that others may learn and benefit from your issue, to respond directly to me remove the nospam. from my email address.

=====
<http://www.lonestaramerica.com/>
=====

Use Outlook Express?... Get OE_Quotefix:

It will strip signature out and more

<http://home.in.tum.de/~jain/software/oe-quotefix/>
=====

Keep a back up of your OE settings and folders with OEBackup:

<http://www.oehelp.com/OEBackup/Default.aspx>
=====