

Re: DNS Server with 2 NICs

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2004-06/0623.html>

From: Ace Fekay [MVP] (*PleaseSubstituteMyActualFirstNamehotmail.com*)

Date: 06/28/04

Date: Sun, 27 Jun 2004 20:34:44 -0400

In news:ushNI9GXEHA.2844@TK2MSFTNGP12.phx.gbl,
Kevin D. Goodknecht Sr. [MVP] <admin@nospam.WFTX.US> posted their thoughts,
then I offered mine

- > *In news:21f6d01c45c1f\$a098da50\$a501280a@phx.gbl,*
- > *Younis Ibrahim <anonymous@discussions.microsoft.com> posted a question*
- > *Then Kevin replied below:*
- >> *I am having a Windows Server 2003 ENT. Running DNS, this*
- >> *machine is having 2 Network Cards, one NIC is having a*
- >> *Public IP and the other one is having Private IP.*
- >
- > *Is this an Active Directory domain?*
- > *Is the AD domain name the same as your public domain name? (if it is*
- > *this is the problem)*
- >
- >
- >> *Now, the problem I am facing is that when I ping my DNS*
- >> *from outside I keep on getting the Private IP, and not*
- >> *the public one?!!!*
- >
- > *If you are trying to host the public zone on the private DNS server*
- > *with Active Directory, you must give your AD Domain a different name*
- > *from the public domain. This is not going to be an easy task and will*
- > *take a complete understanding of Active Directory and how it relies*
- > *on DNS. Your AD domain must resolve to addresses that its members can*
- > *connect to without fail. If the AD domain is behind NAT and has a*
- > *private address scheme, then DNS must always return Private addresses*
- > *for the DCs so the internal clients can find it. If DNS returns a*
- > *public IP for the DCs name your internal clients will not be able to*
- > *connect to the DC to authenticate.*
- >
- >> *How can I stop this?? I want to still be able to allow my*
- >> *clients internally to connect to the private ip from*
- >> *inside.*
- >
- > *You will need to give your AD domain a name that can only resolve to a*
- > *private IP address. Then you are going to need to make some registry*
- > *entries to keep the DC from registering the public addresses in the*

> private zone. If you do not do this you are always going to have
> problems with both public and private sides of the domain.
> e.g. the internal AD domain needs to be something like
> "mydomain.local" or "<localname>.mydomain.com". Either of these will
> work because they will only resolve to local addresses for the AD
> domain members to use to connect to the DC.
>
>
>> When I remove the "Everyone" group from the "A" Record of
>> Private IP, it automatically removes the same from the
>> Public one, which disallows pinging from outside.
>>
>> How can I solve this? Appreciate your help guys.
>
> Either change your AD domain name or set up two different DNS
> servers, one for the internal clients and one for the external
> clients.
> Your problem is identical to Darrel's in these previous threads. He
> changed his internal domain name and after making a few adjustments
> his public domain and AD domain are happily coexisting on the same
> DNS server.
>
>
> Multihomed DNS Server Mailserver Webserver Fileserver
> news:9f27bee2.0406041356.421bf66d@posting.google.com
>
> Intermittent Internet Connection – DNS Netlogon refresh problem?
> news:ez2fA7xUEHA.3332@tk2msftngp13.phx.gbl
>
>
> --

Just want to add, if he's hosting his public name on his DNS, then he needs a separate physical server just for the public records if he's got a split horizon scenario (same name internal/external).

--

Regards,
Ace

Please direct all replies to the newsgroup so all can benefit.
This posting is provided "AS-IS" with no warranties and confers no rights.

Ace Fekay, MCSE 2000, MCSE+I, MCSA, MCT, MVP
Microsoft Windows MVP - Active Directory

HAM AND EGGS: A day's work for a chicken; A lifetime commitment for a pig. --

=====