

# Re: Unix Bind and Windows DNS with Dynamic update issues!!!

---

*Source:*

<http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.dns/2005-05/msg00103.html>

---

- *From:* "Mugen" <[Mugen@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Mugen@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 9 May 2005 10:59:01 -0700
- 

Hi,

>>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.)
- 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)

I know it would be a "Perfect World" if i do all this. But the FACT is that we are running UNIX BIND as internal and external DNS server. All of our internal clients like Windows, Mac etc are pointing to UNIX BIND server to resolve internal hostname and internat name.

What can i do to accomplish this? I setup a Windws DNS server created 6 zones files in UNIX and Windows (\_TCP, \_UDP, MSDCS, \_SITES etc) and just for SRV records resolution. But i can only make it work if i put Windows DNS server address in Windows DNS clients entrie (able to join AD Domain but not dynamically updating clients hostanme in Windows DNS).

Can ANYONE really help with this? I am just stuck here.

Thanks.  
Mugen

"Herb Martin" wrote:

> "Mugen" <[Mugen@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:Mugen@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message  
> <[news:D4CE1EB2-6F24-40B9-A790-B592CEA6229B@xxxxxxxxxxxxxxxxxxxxx](mailto:news:D4CE1EB2-6F24-40B9-A790-B592CEA6229B@xxxxxxxxxxxxxxxxxxxxx)>  
>> Currently, I have a network running NT 4.0 with WINS only, but use a UNIX  
> DNS  
>> server for internal and external name resolution. The plan is to upgrade  
> to

## Re: Unix Bind and Windows DNS with Dynamic update issues!!!

>> Windows 2003/AD, but the Unix DNS server  
>> still needs to be in place and all of our Windows clients are pointing to  
>> Unix for DNS resolution. The plan is to call our new forest root domain  
>> "company.com"  
>> the same name that the Unix DNS server is the authoritative server for that  
>> domain.  
>  
> You might wish to reconsider that name decision, although  
> I myself frequently use it. Your internal users will not be  
> able to address your web server using the 'base' name of the  
> domain (e.g., domain.com) but will require the www prefix  
> (e.g., www.domain.com) since all of the DCs register the  
> base name and interfere.  
>  
>> Now, I have setup a Windows 2003 AD and DNS test server with same FQAN  
>> "company.com" as UNIX (Unix is the root authoritative domain for  
>> "company.com"). I added Windows 2003 DNS as a third DNS entry in Windows  
>> clients in order for Windows clients to join AD Domain and search AD  
> objects.  
>  
> All of your clients must use ONLY DNS servers that return a  
> complete and consistent set of answers. In practice this means  
> the internal DNS server set that is dynamic and support the  
> AD domain name.  
>  
>> (Otherwise Windows clients will not able to join AD Domain)  
>  
> Right. And will authenticate badly or not at all.  
>  
>> But the problem i have right now is Dynamic update is not working in  
> Windows  
>> DNS server unless i change the order of Windows DNS server as Primary  
> option.  
>  
> Even then it will not be reliable. You must NOT depend on client  
> "order" to make things work — it is not reliable (nor ever intended  
> to be reliable.) DNS clients assume that all of their DNS servers  
> will return the SAME (and correct) answers.  
>  
> Your BIND server must either be the ONLY Primary for this (internal)  
> zone and be dynamic, or it must become a Secondary to the AD Dynamic  
> DNS zone, or none of your internal clients may use the BIND server  
> on their NIC client properties.  
>  
>> Is that true i have to make Windows client pointing to Windows DNS server  
> as  
>> Primary option in order to make dynamic update working?  
>  
> No, not precisely. The above statement is an over-specific  
> interpretation of what I wrote in the previous paragraph:  
>

## Re: Unix Bind and Windows DNS with Dynamic update issues!!!

- > The INTERNAL clients must use strictly the INTERNAL DYNAMIC
- > DNS servers --- no matter which machines do that.
- >
- >> But i really need to
- >> have Windows clients pointing to UNIX as Primary/Secondary choice.
- >
- > Why? (Truth is you do not in all likelihood need to do that.)
- >
- > The internal DNS will forward to the UNIX or other DNS server
- > to handle Internet lookups.
- >
- > Whether the "BIND" server is part of that internal DNS server
- > set is an option --- probably easiest not to do that, but still an
- > option.
- >
- >> Any suggestion would be appreciate!
- >
- > Completely separate your internal from your external DNS.
- >
- > In fact, your external DNS is best placed back at the REGISTRAR
- > for all but the largest (in terms of Internet presence) companies.
- >
- >
- > Here are the basic guidelines and checks to ensure with DNS for AD.
- > (Note there is no "requirement" for removing BIND, the requirements
- > are in terms of the functions and information of the various DNS
- > servers.)
- >
- > 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.)
- > 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

