

Re: Need help with DNS design and settings

Source: <http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.dns/2004-09/0052.html>

From: Mark Renoden [MSFT] (markreno_at_online.microsoft.com)

Date: 09/01/04

Date: Thu, 2 Sep 2004 09:02:22 +1000

Hi

2. Stubs can be whatever you like. AD Integrated vs not AD Integrated is just a question of where it's stored and you can use this to define the scope of servers ... all DC's or all DNS servers etc.

3. AFAIK the default replication scope is to all DNS server in the forest for the `_msdcs.<forestroot>` zone. It needs to be visible to all forest members so this makes sense. All DNS servers in the forest have a copy and then all clients that query their local domain DNS server can see it.

I think your reverse lookup zone question was answered.

Kind regards

--

Mark Renoden [MSFT]

Windows Platform Support Team

Email: markreno@online.microsoft.com

Please note you'll need to strip ".online" from my email address to email me; I'll post a response back to the group.

This posting is provided "AS IS" with no warranties, and confers no rights.

"Slater" <slaterlovesspam@yahoo.com> wrote in message

news:JXlZc.641\$TH6.281@fel.columbus.rr.com...

> Re: #1 - OK, that makes sense.

>

> Re: #2, can or should you have stub zones with AD-integrated DNS? I didn't think you could.

>

> I'm not sure what you mean on #3. I thought the default setting in Server 2003 on ALL zones was to replicate to "All DCs in the domain" (the third option)?

>

> Finally, a new question - after describing my small network, do you feel I need reverse lookup zones? Everywhere I read say they are not necessary, but

> to me they make sense because a lot of times you resolve names from IPs (I know I do as the sysadmin). What are the cases when you should run reverse lookup zones - large companies with dozens of domains and sites?

>

> - Slater

>

>

> "Mark Renoden [MSFT]" <markreno@online.microsoft.com> wrote in message

Re: Need help with DNS design and settings

microsoft.public.win2000.dns: Re: Need help with DNS design and settings

```
> news:O$iu8i9jEHA.3912@TK2MSFTNGP12.phx.gbl...
>> Hi
>>
>> On point 1, you understand me correctly and it certainly can't hurt to
> have
>> the alternate set. The way it works is that the preferred is used until
> it
>> doesn't response (note that this is different to a negative response).
> When
>> there is no response, we start using the alternate until it doesn't
> respond.
>> We then toggle back to the primary.
>>
>> In troubleshooting issues for customers, we often point all servers at
>> the
>> same DNS server for the primary and reboot so that they have a consistent
>> view of DNS. I can't think of any good reason for never using an
> alternate
>> provided all DNS servers have a consistent copy of the zone. Under
> Windows
>> 2000, there was actually an issue with pointing DC's to themselves for
>> DNS
>> in the forest root domain (islanding). As far as I know, Microsoft has
>> resolved this in 2003.
>>
>> 2. Name server box is only the servers authoritative for that zone.
> You'll
>> notice it's a tab on the properties of the specific zone. Just leave it
>> alone and you should be OK.
>>
>> Conditional forwarding will work. I just think it's more administrative
>> overhead and stub zones are self updating. If you add or remove a DNS
>> server, the SOA's get updated.
>>
>> 3. Forgot to mention the _msdcs.<forestroot> zone. Under Windows Server
>> 2003, the default is that the zone replicates to all DNS servers in the
>> forest. This is a good thing. Everyone needs access to this zone.
>>
>> HTH
>> --
>> Mark Renoden [MSFT]
>> Windows Platform Support Team
>> Email: markreno@online.microsoft.com
>>
>> Please note you'll need to strip ".online" from my email address to email
>> me; I'll post a response back to the group.
>>
>> This posting is provided "AS IS" with no warranties, and confers no
> rights.
>>
>>
>>
>> "Slater" <slaterlovesspam@yahoo.com> wrote in message
>> news:3oaZc.57985$cT6.10329@fe2.columbus.rr.com...
>> > On 1, are you saying the DNS server should point to itself as the
> primary,
>> > and a second DNS server in the same domain as a secondary (in my
>> > example
> I
>> > have 2 DNS servers per domain, so each one would list the other as the
>> > secondary)? If so, that goes against everything I have ever read. In
> fact,
```

microsoft.public.win2000.dns: Re: Need help with DNS design and settings

```
>> > when you use the Microsoft wizard, it sets up the DNS server as the
>> > primary
>> > with no secondary. I agree with your reasoning, but everyone else must
>> > always say to set it up by itself for a reason...
>> >
>> > As far as 2, yes the name servers for each domain do get populated. I
>> > am
>> > confused if I should basically list every name server in my entire
> forest
>> > in
>> > the name server box on every DNS server (in my example, there would be
>> > 4
>> > DNS
>> > servers total, 2 for each domain. So should I list all 4 servers in the
>> > name
>> > server box on all 4 machines?) I was thinking this would help the
> servers
>> > "find" one another. Or does the name server box list the servers that
> are
>> > authoritative for that domain only?
>> >
>> > Also on #2 what's your opinion on the conditional forwarding I was told
> to
>> > do? This is an alternative to stub zones I believe and is supposed to
> help
>> > requests for addresses in another domain easier to locate. For example,
> if
>> > a
>> > user in root.priv asks the root.priv DNS server for the address of a
>> > machine
>> > in corp.priv, the root.priv DNS server would forward the request to the
>> > corp.priv DNS server. Correct? Again, the concept sounds logical but I
>> > just
>> > wanted to make I was setting everything up right.
>> >
>> > I understand #3 - makes sense.
>> >
>> > Thanks,
>> > - Slater
>> >
>> >
>> > "Mark Renoden [MSFT]" <markreno@online.microsoft.com> wrote in message
>> > news:ewSxx$7jEHA.1656@TK2MSFTNGP09.phx.gbl...
>> >> Hi
>> >>
>> >> Just to clarify, we're not talking about parent child domains, we're
>> >> talking
>> >> about forest root and tree root domains. The way you handle these is
>> >> different. For your forest root / tree root domain setup ...
>> >>
>> >> 1. It's normally good to point the DC/DNS server to itself and to
> another
>> >> DC/DNS server in the same domain as alternate. This way, if the DNS
>> >> service
>> >> fails for any reason locally, you've got the alternate you can make
>> >> requests
>> >> to.
>> >>
>> >> 2. The name servers box is usually populated automatically (at least I
>> >> thought so) with the DNS servers you have the AD integrated zones on.
> So
>> >> for example, the root.priv AD integrated zone, you should see the two
```

microsoft.public.win2000.dns: Re: Need help with DNS design and settings

```
>> > DC/DNS
>> >> servers that exist in that domain listed there.
>> >>
>> >> You want to forward to your BIND servers for external resolution in
> both
>> >> domains. To resolve names from one domain to another, consider
> secondary
>> > or
>> >> stub zones (this are kewl in 2K3).
>> >>
>> >> 3. Clients should point to the DC/DNS servers in their own domain with
>> >> the
>> >> preferred server in the same site.
>> >>
>> >> HTH
>> >> --
>> >> Mark Renoden [MSFT]
>> >> Windows Platform Support Team
>> >> Email: markreno@online.microsoft.com
>> >>
>> >> Please note you'll need to strip ".online" from my email address to
> email
>> >> me; I'll post a response back to the group.
>> >>
>> >> This posting is provided "AS IS" with no warranties, and confers no
>> > rights.
>> >>
>> >> "Slater" <slaterlovesspam@yahoo.com> wrote in message
>> >> news:PT4Zc.268401$fv.189161@fe2.columbus.rr.com...
>> >> > I've been an NT4 admin for years and am responsible for migrating us
> to
>> >> > 2003. I'm new to AD and am certainly no expert on AD or DNS, but I
> have
>> >> > read
>> >> > MS books, Mark Minasi's 2003 book, and the O'Riely 2003 DNS book.
>> >> > All
>> >> > of
>> >> > the
>> >> > books and scenerios all seem to just discuss simple AD setups. I had
> a
>> >> > test
>> >> > AD working for months using 2000 and it worked great but that was a
>> > single
>> >> > domain. I started over with 2003 this time and now that I am trying
> to
>> > add
>> >> > a
>> >> > child domain (i.e. domain tree) I am having some problems and no one
>> > seems
>> >> > to cover this scenerio to the point where I understand it. I
> understand
>> >> > the
>> >> > CONCEPTS just fine - it's when you get to the nuts and bolts of what
>> >> > settings go where that everyone seems to leave that out of all of
>> >> > the
>> >> > training material.
>> >> >
>> >> > Here's the setup - Each domain will have 2 DCs. The DCs will run
>> > Microsoft
>> >> > DNS and be AD-integrated. One domain (root.priv) will be an empty
> root
>> >> > domain for the sole purpose of isolating the Enterprise admin
```

microsoft.public.win2000.dns: Re: Need help with DNS design and settings

```
>> >> > account
>> > and
>> >> > making it easier down the road to reshape the forst if we ever need
> to.
>> >> > The
>> >> > second domain (corp.priv) will be the actual production domain that
> all
>> >> > 100
>> >> > of my users will belong to and use. It's just a separate tree in the
>> >> > forest.
>> >> > I also have 2 caching BIND DNS servers on the outside interface for
>> >> > internet
>> >> > queries, which I will slave my internal DNS servers to for external
>> > query
>> >> > forwarding. Each DC will be a GC server, and one DC in each domain
> will
>> > be
>> >> > located offsite for disaster recovery purposes (P2P VPN connection
>> > between
>> >> > the sites). That's pretty much it, other than I need to run WINS in
> the
>> >> > corp.priv domain. The corp.priv domain will be divided into 2
>> >> > network
>> >> > subnets (the second subnet is a QA network that is currently an NT4
>> > domain
>> >> > but I will just make it an OU in the corp.priv domain once I
> migrate).
>> > So
>> >> > my
>> >> > plan was to have a DHCP server in the corp.priv domain that will
>> >> > give
>> > out
>> >> > addresses in 2 different subnets (we have DHCP relaying enabled on
> our
>> >> > cisco
>> >> > routers). Sounds easy enough on paper, but once I tried to build it
>> >> > I
>> >> > am
>> >> > having problems with DNS. I've been trying a bunch of things but
>> >> > it's
>> >> > getting down to crunch time and it's starting to tick me off.
>> >> >
>> >> > Here's where I'm confused:
>> >> >
>> >> > 1. Local TCP/IP settings on the DNS servers:
>> >> >
>> >> > I'm confused how to fill out each DC/DNS server's TCP/IP settings.
> For
>> >> > example, in the local TCP/IP properties, I know that all DNS servers
>> >> > should
>> >> > point to themselves as the primary and no secondary, so that's what
>> >> > I've
>> >> > done on all of the servers (I used the actual IP of the box, not
>> > 127.0.0.0
>> >> > like Microsoft says to do). But I don't know if the same "point to
>> > itself
>> >> > as
>> >> > the primary w/no secondary" rule applies for the corp.priv domain's
> DNS
>> >> > servers as well.
>> >> >
>> >> > 2. The DNS settings:
```

microsoft.public.win2000.dns: Re: Need help with DNS design and settings

```
>> >> >
>> >> > What goes in the name servers box? Do you just list each name server
> in
>> >> > that
>> >> > domain, or do you list EVERY name server in your forest in every DNS
>> >> > server's name server box? For example, on the root.priv DNS servers
> do
>> >> > I
>> >> > just list the 2 root.priv servers, and on the corp.priv DNS servers
>> >> > list
>> >> > the
>> >> > corp.priv servers? Or do I need to instead list all 4 DNS servers on
>> > each
>> >> > DNS server?
>> >> >
>> >> > What goes in the forwarders box? Since I want to be slaved to
> external
>> >> > forwarders for internet queries, I put the address of my 2 external
> DNS
>> >> > servers in the forwarders box for "all other DNS domains" and
>> >> > checked
>> > the
>> >> > "do not use recursion for this domain" checkbox. This worked great
>> >> > on
>> > the
>> >> > root.priv DNS servers, but do I do the same on the corp.priv
>> >> > servers?
>> >> > Basically I want ANY internet query from ANY internal dns server to
> be
>> >> > slaved to external forwarders. But I don't understand if child
>> >> > domain
>> > DNS
>> >> > servers are even supposed to resolve internet queries themselves, or
> if
>> >> > child domain DNS servers are supposed to forward all DNS queries
>> > (internal
>> >> > or external) to its parent's DNS server?
>> >> >
>> >> > And how does root.priv and corp.priv forward queries to one another?
>> >> > Someone
>> >> > recommended to me that I use conditional forwarding. For example, on
>> >> > the
>> >> > forwarders tab of the root.priv DNS servers, create a new corp.priv
>> > domain
>> >> > and list the corp.priv's DNS servers. And do the opposite for the
>> >> > corp.priv
>> >> > DNS servers. Is this correct and do I check the "do not use
>> >> > recursion
>> > for
>> >> > this domain" checkbox like I did for the external slave forwarders?
>> >> >
>> >> > 3. Client TCP/IP settings:
>> >> >
>> >> > What DNS server would clients point to as their primary and
>> >> > secondary
>> > DNS
>> >> > servers? Should machines in Root.test point to the root.test dns
>> > servers,
>> >> > and the machines in corp.test point to the corp.test dns servers? Or
>> >> > should
>> >> > everyone point to the root.test dns servers? Or does it matter?
>> >> >
```

microsoft.public.win2000.dns: Re: Need help with DNS design and settings

```
>> >> > =====  
>> >> >  
>> >> > Is there any other tricks I need to do on the 4 DC/DNS servers? A  
>> >> > microsoft  
>> >> > article I found said to add the IP addresses (and domain name  
>> >> > instead  
>> >> > of  
>> >> > the  
>> >> > server name) of the DCs to the host file on each DC. This supposedly  
>> > helps  
>> >> > with DNS resolution issues and some AD replication problems I was  
>> > having.  
>> >> > Is  
>> >> > there any other tips from veterans like this I need to know about to  
>> > make  
>> >> > my  
>> >> > life easier?  
>> >> >  
>> >> > Any assistance is greatly appreciated. I know DNS is the heart of  
>> >> > AD,  
>> > and  
>> >> > if  
>> >> > that's not worknig then everything else will just be fubarred. So I  
>> >> > want  
>> >> > to  
>> >> > make sure all of my t's are crossed and i's are dotted before going  
>> >> > forward  
>> >> > with any of the NT4 migration procedures and everything else.  
>> >> >  
>> >> > I am free to design things however I see fit, so if anyone has a "if  
> I  
>> > was  
>> >> > going to do it here's what I would do" idea I would love to hear it  
>> >> > too.  
>> >> >  
>> >> > - Greg  
>> >> >  
>> >> >  
>> >>  
>> >>  
>> >  
>> >  
>>  
>>  
>  
>  
>
```