

## Re: Active Directory and child DNS Zone

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2004-08/0135.html>

---

**From:** Mark Renoden [MSFT] (*markreno\_at\_online.microsoft.com*)

**Date:** 08/06/04

Date: Fri, 6 Aug 2004 12:14:07 +1000

Hi Mike

The configuration that you've currently got should work. The issue comes when you can't guarantee internal clients won't try to access your external facing web servers. I'm not sure it's regarded "best practice" to do what I've suggested. I think it's just generally accepted as simpler to manage, especially if you manage your own external DNS name space.

Many companies use *companyname.com* externally and *corp.companyname.com* internally (or something similar).

Kind regards

--

Mark Renoden [MSFT]

Windows Platform Support Team

Email: [markreno@online.microsoft.com](mailto: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.

"Mike C" <[MikeC@discussions.microsoft.com](mailto:MikeC@discussions.microsoft.com)> wrote in message

news:6E0DB4BE-73E7-4294-BFA2-EC89B05D2909@microsoft.com...

> Thanks Mark, that does make sense.

>

> But, having said that, I must add a couple more pieces of information.

> Our internal and external DNS domains are both the same - *mycompany.com*.

> But, there is NO DNS communications between the two domains. Our ISP

> hosts our external domain and it only contains entries for our web servers

> in our DMZ. We do not allow DNS packets to go from our internal network

> to the external. The only external access is granted through web proxy

> for browser use and our ISA server does the lookups.

>

> I don't foresee this configuration changing, but I guess that is a

> possibility for the future. Is it still recommended best practice to

> specify an AD forest name different than our current DNS namespace? Even

> if the two should never meet?

>

> Mike

>

>

> "Mark Renoden [MSFT]" wrote:

>

>> Hi Mike

## microsoft.public.windows.server.dns: Re: Active Directory and child DNS Zone

```
>>
>> Basically, the reason is this ...
>>
>> If your registered name is owned by the DNS servers you have in your
>> environment and they are world visible (ie ... they handle your internet
>> presence), you don't want your internal AD domain to register records in
>> that zone. If you do, those records end up being world visible also.
>> The
>> less you expose to the world, the better.
>>
>> It's not even necessary to use a child domain. You could use something
>> like
>> companyname.local or companyname.corp. Provided you configure all
>> clients
>> in the domain to use the DNS servers which control that zone and that you
>> configure forwarders appropriately, this is perfectly valid. Your
>> internal
>> name space does not have to have anything to do with your external name.
>>
>> 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.
>>
>> "Mike C" <Mike C@discussions.microsoft.com> wrote in message
>> news:562A334B-465B-4946-A8BF-6D5A70ED510E@microsoft.com...
>> > I'm looking at migrating an NT 4.0 Domain to Windows 2003 Active
>> > Directory. Currently we run DNS on Windows 2000 member servers. Our
>> > plan
>> > is to upgrade the NT 4.0 Domain controller to Windows 2003 and install
>> > active directory on it.
>> >
>> > Our registered DNS name is companyname.com and everything that I have
>> > read
>> > tells me I must create a child DNS zone ( ie ad.companyname.com ) to
>> > house
>> > my AD root. Is this necessary or just best practice? In a test bed, I
>> > migrated to AD, told the DC to use mycompany.com as the root DNS and
>> > pointed to the Windows 2000 DNS servers. Everything seemed to work ok,
>> > but the test bed isn't a true picture ( no internet access to test VPN,
>> > etc ).
>> >
>> > Is there documented reasoning behind installing AD in a child DNS
>> > domain
>> > as opposed to using an existing DNS zone?
>> >
>> > Thanks
>>
>>
>>
```