

## Re: AD DNS naming

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2006-03/msg00447.html>

---

- *From:* "SuperGumby [SBS MVP]" <[not@xxxxxxxxxxx](mailto:not@xxxxxxxxxxx)>
  - *Date:* Fri, 24 Mar 2006 09:08:38 +1100
- 

G'day Ace,

Nice breakdown.

I suppose my main concerns stem from questions raised where the DNS naming has been assumed ('it's asking for a DNS name, better give it this one') rather than planned.

If I juggle the info around somewhat I get 'considerations that should influence your AD DNS name choice':

(in no particular order)

Security.

Considerations about what info from the DNS is exposed by the different choices when implemented properly or improperly.

Name complexity.

`we.dont.wanna.have.to.remember.something.like.this` to access a record.

User considerations, the 'people' aspect. Some consideration here for the 'machine' context.

Name visibility.

How does resource availability differ inside vs outside the AD?

Also, from other post, what differing visibility do I wish to provide and is this dependent on the choice.

Managability.

Does the choice influence the amount of work necessary to maintain the system?

I have to go play golf in a few minutes. It will give me time to think about what other aspects I want to consider in the process of choosing the name. I'll pop back in to see what else comes in.

"Ace Fekay [MVP]"

<[PleaseSubstituteMyActualFirstName&LastNameHere@xxxxxxxxxxx](mailto:PleaseSubstituteMyActualFirstName&LastNameHere@xxxxxxxxxxx)> wrote in message [news:%233spY\\$TGHA.4340@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%233spY$TGHA.4340@xxxxxxxxxxxxxxxxxxxxxxxx)

In [news:OO9hT9ZTGHA.4956@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OO9hT9ZTGHA.4956@xxxxxxxxxxxxxxxxxxxxxxxx),

SuperGumby [SBS MVP] <[not@xxxxxxxxxxx](mailto:not@xxxxxxxxxxx)> stated, which I commented on below:

Re: AD DNS naming

Hi,

I have a problem I believe this group can help me with, in regard to AD DNS naming. Thing is, I don't have an immediate problem which anyone needs to work on, it is more that I am after opinions, discussion, and, well, argument (in the proper sense of the word, not screaming matches).

My name's Mick Malloy and as you may guess from my moniker I'm an SBS (Small Business Server) MVP. I became an MVP through involvement in newsgroups and that is what has led me here. In search of an answer to my question I've gone a fair way back into previous posts and 'lurked' for the last few days, but really I find little discussion about my point of interest.

My interest is discussion of the pros and cons of naming your AD DNS .local vs a name related to your FQDN. I'm using .local here as a bit of a generalisation, I actually prefer .lan due to the special handling some OS's (OSX and a couple of Linux variants) use for the .local domain but if we discount special handling or start from a premise of .whatever (as long as it is not related to your internet FQDN) you are likely to understand where I'm coming from.

/cards on the table time

I believe it is wrong to name your AD DNS with any relationship to your internet FQDN. It is wrong to name your AD DNS company.com and it is only slightly less wrong to name it branch.company.com.

I believe most people approach the question from the wrong angle, 'I have this name (FQDN), I think I'll use it for my AD DNS.' where I believe they should rather ask 'I need to create an AD DNS name, is there any reason why it should relate to my public FQDN or should I use a different namespace?'

Pointers to previous discussion will be appreciated, and read.  
Your participation in new discussion will be greatly appreciated.

TIA  
MM

Hi Mike. Good to see a fellow MVP posting. :-)

I must say this is a classic question that stems back to the beginning days of AD. Naming your internal domain name can be based on a number of things, whether technical or political, or previous administrative experience. This has been highly discussed (not debated) in the past. Whatever decision you make for an AD DNS FQDN domain name, just understand the ramifications. Actually I'm not going to try to get into any sort of debate, for there is really nothing to debate, nor help someone decide on what is 'right' or 'wrong' but rather just state the implications and how to get around them, no matter what the decision was based on.

Re: AD DNS naming

=====  
The passage below is a compilation of a discussion between myself and Todd J. Heron, MVP, from exactly one year ago to this date.  
=====

Classic question:

"Which are the advantages of naming my domain with domain.com rather than domain.local? I have a domain.com registered for my Company that i use for my e-mail and Site Internet."

There are different answers to this classic question and while these answers ultimately depend upon company preference, much of the direction will be based upon administrator experience. The three basic scenarios outlined below are the most commonly given answers to the question, sometimes altogether and sometimes not. Some company networks use a combination of these scenarios. When explaining it to a relative beginner asking the question, many responses omit explanatory detail about all the scenarios, for fear of causing more confusion.

All three approaches will have to take both security and the end-user experience into perspective. This perspective is colored by company size, budget, and experience of personnel running Active Directory and the network infrastructure (mostly with respect to DNS and VPN). No one approach should be considered the best solution under all circumstances. For any host name that you wish to have access from both your internal network and from the external Internet you need scenario 1, although it is the most DNS-intensive over time. If you do not select this option and go with scenario 2 or 3 only, consideration will have to be given to the fact that company end-users will need to be trained on using different names under different circumstances (based on where they are (at work, on the road or at home)).

=====  
Scenario 1.

Choosing the same name internal/external (spilt-zone, or split-brain, whatever you want to call it) has the most administrative overhead. Why chosen? Either because a misunderstanding of the pros/cons, political, or for ease of use.

Pros:

1. Their email address is their logon name. Easier to remember.
2. Security. Each DNS zone is authoritative for the zone of that name so therefore the external DNS zone and internal AD/DNS zone will NOT replicate with each other thereby prevent internal company records to be visible to the outside Internet.
3. Short namespace. Users don't have to type in (or see) a long domain name when accessing company resources either internally or externally. Names are "pretty".

## Re: AD DNS naming

### Cons:

1. Administrative overhead. If trying to get to your externally hosted website, it won't resolve because a DNS server will not forward or resolve outside for what a zone that it hosts. You can overcome resolving the www.domain.com dilemma by using a delegation. Rt-click your zone, new delegation, type in 'www' and provide the public SOAs for the nameserver(s). This way it will send the resolution request to the SOA and resolve that way. As for <http://domain.com>, that is difficult and would instruct all users to only use www.domain.com. This is because of the LdapIpAddress, the record that shows up as (same as parent), which EACH domain controller registers. So if you type <http://domain.com>, you will round robin between the DCs. To overcome that, on EACH DC, install IIS, then under the default website properties, redirect it to www.domain.com and let the delegation handle it. Now if you were to be using Sharepoint services, or something else that connects to the default website (no sub folders or virtual directories), then it becomes a problem. I know numerous installations setup with this and have operated fine for years.
2. Security. Each DNS zone is authoritative for the zone of that name so therefore the external DNS zone and internal AD/DNS zone will NOT replicate with each other thereby prevent internal company records to be visible to the outside Internet.
3. Any changes made to the public DNS zone (such as the addition or removal of an important IP host such as a web server, mail server, or VPN server) must added manually to the internal AD/DNS zone if internal users will be accessing these hosts from inside the network perimeter (a common circumstance).
4. VPN resolution is problematic at best. Company users accessing the network from the Internet will easily be able to reach IP hosts in the public DNS zone but will not easily reach internal company resources inside the network perimeter without special (and manual) workarounds such as maintaining hosts files on their machines (which must be manually updated as well everytime there is a change to an important IP host in the public zone), entering internal host data on the public zone (such as for printers, SRV records for DCs, member server hosts, etc), which exposes what internal hosts exist, or they must use special VPN software (usually expensive), such as Cisco, Netscreen, etc, which is more secure and reliable anyway.

For further reading on this scenario:

[http://www.isaserver.org/tutorials/You\\_Need\\_to\\_Create\\_a\\_Split\\_DNS.html](http://www.isaserver.org/tutorials/You_Need_to_Create_a_Split_DNS.html)

<http://homepages.tesco.net/~J.deBoynePollard/FGA/dns-split-horizon-common-server-names.html>

=====

### Scenario 2.

Choosing a child name or delegated sub domain name of the public zone. This is one recommendation. Name such as 'ad.domain.com', or 'corp.microsoft.com'. The AD DNS domain name namespace starts at

## Re: AD DNS naming

corp.domain.com and has nothing to do with the domain.com zone.

### Pros:

1. Minimal administrative overhead.
2. Forwarding will work.
3. The NetBIOS name will be 'AD' or 'CORP', depending on what you chose and what the users will see in the three-line legacy security logon box.
4. Like Scenario 1, this method also isolates the internal company network but note this at the same time is also a disadvantage (see below).
5. Better than Scenario 1, internal company (Active Directory) clients can resolve external resources in the public DNS zone easily, once proper DNS name resolution mechanism such as forwarding, secondary zones, or delegation zones are set up.
6. Better than Scenario 1, DNS records for the public DNS zone do not need to be manually duplicated into the internal AD/DNS zone.
7. Better than Scenario 1, VPN clients accessing the internal company network from the Internet can easily navigate into the internal subdomain. It is very reliable as long as the VPN stays connected.

### Cons:

1. Confusion on users if they decide on using their UPN.
2. While there is security in an isolated subdomain, there is potential for exposure to outside attack. The potential for exposure of internal company resources to the outside world, lies mainly in the fact that because when the public zone DNS servers receives a query for subdomain.externaldnsname.com, they will return the addresses of the internal DNS servers which will then provide answers to that query.
3. Longer DNS namespace. This may not look appealing (or "pretty") to the end-users.
4. Security. We are assuming that we can only access the internal servers thru a VPN and assuming they are in a private subnet, they won't be accessible. Also assuming to secure the VPN with an L2TP/IPSec solution and not just a quick PPTP connection. If this is all so, we can assume it is secure and not accessible from the outside world.

The scenario is the recommendation from the Windows Server 2003 Deployment Guide. It states to the external registered name and take a sub zone from that as the DNS name for the Forest Root Domain:

<http://www.microsoft.com/resources/documentation/windowsserv/2003/all/deployguide/en-us/default.asp>

=====

Re: AD DNS naming

Scenario 3. Choosing a different TLD: Choosing a different TLD, such as domain.local, domain.corp, domain.net, etc. This option is usually best for either beginners or the expert, because it's the easiest to implement primarily because it prevents name space conflicts from the very beginning with the public domain and requires no further action on your part with respect to that.

But this option does makes VPN resolution difficult (like option 1) and Exchange headers when examined closely will show the company internal AD name which looks unprofessional. You can use any extension you want here such as .ad, .int, .lan, etc...

Pros:

- 1. Easy to implement with minimal administrative overhead. Requires minimal action on administrators.
- 2. Prevents name space conflicts with external domain name.
- 3. Forwarding works.

Cons:

- 1. Domain name may look unprofessional.
- 2. VPN resolution difficult (like option 1). That can be a sticky issue and depending on the VPN client will dictate whether it will work or not. I know one of the other MVPs (Dean Wells) created a little script to populate a user's laptop or home PC's hosts file with the necessary resources and would remove them once the VPN is dissolved.
- 3. Exchange HELO name must be altered (to accomodate anti-spam, SPF, and RBL software), via MetaEdit, Metabase Explorer and thru the SMTP VS properties.

=====

For a broad overview of this entire topic, see below.

DNS Namespace Planning

<http://support.microsoft.com/default.aspx?scid=kb:en-us:254680>

Assigning the Forest Root Domain Name:

<http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?u>

=====

I hope that helps

---

Re: AD DNS naming

Ace

This posting is provided "AS-IS" with no warranties or guarantees and confers no rights.

Having difficulty reading or finding responses to your post?  
Instead of the website you're using, I suggest to use OEx (Outlook Express or any other newsreader), and configure a news account, pointing to news.microsoft.com. This is a direct link to the Microsoft Public Newsgroups. It is FREE and requires NO ISP's Usenet account. OEx allows you to easily find, track threads, cross-post, sort by date, poster's name, watched threads or subject.

It's easy:

How to Configure OEx for Internet News

<http://support.microsoft.com/?id=171164>

Ace Fekay, MCSE 2003 & 2000, MCSA 2003 & 2000, MCSE+I, MCT, MVP  
Microsoft MVP – Directory Services  
Microsoft Certified Trainer

Infinite Diversities in Infinite Combinations  
Assimilation Imminent. Resistance is Futile  
"Very funny Scotty. Now, beam down my clothes."

The only thing in life is change. Anything more is a blackhole consuming unnecessary energy. – [Me]