

Re: Domain naming strategies

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-07/msg00519

- *From:* "Anthony" <anthony.spam@xxxxxxxxxxxxxxxx>
 - *Date:* Tue, 11 Jul 2006 14:22:09 +0100
-

Thanks Ace, those are the discussions I was referring to.
What with extranets and SSL VPN's I am struggling to see a good reason not to use the delegated sub domain of a public zone (scenario2 below), just because it represents reality. The other two routes don't seem to offer any significant security and make it a bit more complicated to manage.
It is odd that such a fundamental part of the AD design has little good reason one way or the other!
Anthony

"Ace Fekay [MVP]" <PleaseAskMe@xxxxxxxxxxxxxxxx> wrote in message news:OBW1%23avoGHA.3964@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

In news:e6r%23kjfoGHA.1600@xxxxxxxxxxxxxxxxxxxxxxxxxxxx, Anthony <anthony.spam@xxxxxxxxxxxxxxxx> stated, which I commented on below:

This question went astray the first time. Its a well worn question, but I'd like to see if there are any new thoughts on this. I am looking at the naming strategy for a new forest. I am aware of the discussions about the alternative strategies: non-valid; non-public and public domains. I can't see a really good reason not to use the public domain name as the starting off point for AD domain naming. The usual reason for using a private namespace like ad.myco.local is that it won't be released to public dns servers. But if the internal version of myco.com was accidentally released, it would just contain a delegation to an unreachable internal dns server. Not a huge problem. Using a non-public namespace like ad.myco.net keeps things tidy if:
there is a very large public presence at myco.com. It would have to be a very large public presence not to have room for ad.myco.com. Its fine if there is a clear split between internal and external, but gets a bit confusing when it comes to the extranet with partners, customers etc. Should they use support.myco.com or support.myco.net? If you use a public namespace, you need to maintain two versions, the external list of public resources and the internal one. But you already need to maintain two lists if you use a different namespace. Its just that the two lists have two different names. It should not

Re: Domain naming strategies

be too difficult for a dns admin to remember that he has two versions of one list rather than two lists.

So, unless you are very very small, or very very large, I can't see a good reason not just to use the one namespace. Then your security comes down to layers of access control between public and private information, rather than a global internal/external split.

Does anyone have anything new to add?

Anthony

Interesting question that has been around forever and re-hashed since the beta days of Windows 2000. Read thru this old discussion. I'm sure it covers just about everything you'll want to know.

=====
Same name AD DNS domain name and external name (split-zone)
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.

=====
The passage below is a compilation of a discussion between myself (Ace) and Todd J. Heron, MVP, from over a year ago.
=====

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

Re: Domain naming strategies

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".

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

Re: Domain naming strategies

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://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 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.

Re: Domain naming strategies

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>

=====
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

Re: Domain naming strategies

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