

Re: About DNS naming convention for Active Directory

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2005-06/msg00131.html>

- *From:* "Ace Fekay [MVP]" <PleaseSubstituteMyActualFirstName&LastNameHere@xxxxxxxxxxx>
 - *Date:* Wed, 8 Jun 2005 00:35:06 -0400
-

In news:OLIZ3U9aFHA.1088@xxxxxxxxxxxxxxxxxxxxxxxx,
Newbie <newbie@xxxxxxxxxxx> stated, and I replied below:

I'm sorry for jumping all over the places for this AD upgrade for our company. I made a mistake today by plugging the test AD to the corporate network and caused some users not be able to login to their computers.
Simon

We'll try to keep the discussion here so we can collaborate with all the facts.

You stated that you successfully upgraded to Win2003. I am assuming you upgraded your NT4 domain controller to this new 2003 domain controller. All services, such as logon, authentication, etc, should continue as previous under NT4 with the same users.

Now, if I may try to translate what you just posted here, you are saying that you upgraded this in a test network and then plugged it into your main network? I thought you mentioned earlier (as I implied above), that you upgraded your production machine?

What is your current production domain? NT4 or Win2003?

Is the test AD Netbios domain name the same as the production Netbios domain name? That can cause issues if both are side by side with the same Netbios domain name, depending on if you are using WINS, and if you set the test machine to use the production WINS server. Now AD doesn't require WINS to function, since it relies purely on DNS services, but it can affect your current legacy and newer clients, since they've been using NTLM as the authentication method with NT4. Once Win2000 and newer machines realize there's an AD domain out there, their authentication method now turns to and sticks with Kerberos. If they try to authenticate against the NT4 domain, it will fail. If you unplug the AD DC, their authentication attempts will fail. There is an article describing this, and was fixed with later service packs, and not sure if it applies, since I do not know all the facts. Upto now, I do not know your config.

Re: About DNS naming convention for Active Directory

284937 - Windows 2000-Based Clients Connect Only to the Domain Controller That Was Upgraded First in a Mixed-Mode Domain:

<http://support.microsoft.com/?id=284937>

Here's a little snippet from one of my previous posts explaining about AD and DNS: Also, please take the time to read this passage and some of the articles I provided below. They are short and to the point and may help give you a better understanding of how AD and DNS works.

=====

Just a little background: AD uses DNS. DNS stores AD's resource and service locations in the form of SRV records, hence how everything that is part of the domain will find resources in the domain. If the ISP's DNS is configured in the any of the internal AD member machines' IP properties, (including all client machines and DCs), the machines will be asking the ISP's DNS "where is the domain controller for my domain?", whenever it needs to perform a function, (such as a logon request, replication request, querying and applying GPOs, etc). Unfortunately, the ISP's DNS does not have that info and they reply with an "I dunno know", and things just fail..

So you cannot use your ISP's DNS addresses anymore in your client or any other machines. You cannot use your router as a DNS or DHCP server either. If you are using your NT4 as a DNS server, that all needs to be changed over to Win2003 DNS. Same with DHCP. NT4 DNS cannot support AD's SRV requirements and dynamic updates.

If this is the current scenario, it is highly suggested and recommended to only use the internal DNS servers on the network that is hosting the AD zone name. This applies to all machines, (DCs and clients). Believe me, Internet resolution will still work with the use of the Root hints (as long as the root zone doesn't exist).

However, for more efficient Internet resolution, it's recommended to configure a forwarder. If the forwarding option is grayed out, delete the Root zone (looks like a period). If not sure how to perform these two tasks, please follow one of the two articles listed below, depending on your operating system. They show a step by step on how to perform these tasks:

323380 - HOW TO Configure DNS for Internet Access in Windows Server 2003 :
<http://support.microsoft.com/?id=323380>

300202 - HOW TO Configure DNS for Internet Access in Windows Server 2000 :
<http://support.microsoft.com/?id=300202>

DNS and AD (Windows 2000 & 2003) FAQ:

Re: About DNS naming convention for Active Directory

Re: About DNS naming convention for Active Directory

<http://support.microsoft.com/?id=291382>

=====

Do use a favor, to get a more specific picture about your config, can you please post:

1. ipconfig /all of your new DC, your NT4 machine, and one of your DHCP clients.
2. The exact spelling of your zone name in DNS
3. If dynamic updates are enabled in the zone properties
4. Any Event log errors.

Thanks,
Ace

.