

SVR370

Name Resolution 2008 Style: What's up with DNS, WINS, and NetBIOS

Presented by Mark Minasi
help@minasi.com
www.minasi.com
copyright 2008 Mark Minasi

Microsoft®
tech·ed
IT Professionals | 2008

1

Name Resolution News

- ▶ The status of NetBIOS and NetBT
- ▶ Changes to DNS internals
- ▶ Administering DNS in 2008
- ▶ DNS and AD setup in 2008
- ▶ DNS client changes: finding DCs better
- ▶ New DNS resource records (the good stuff)
- ▶ IPv6 Name Resolution

2

2

Is NetBIOS Finally Dead?

- ▶ Nope, apparently not
- ▶ The original plan for 2008 was to turn off NetBIOS over TCP by default
- ▶ That changed
- ▶ But you might just be able to do it yourself
- ▶ You can find it on the WINS tab of IP properties, or you can shut it off via DHCP
- ▶ Test first, of course, but if you're a Windows / Office shop then it'll probably work, and it'll be faster

3

3

WINS?

- ▶ Again, nothing much as far as I can see
- ▶ Clusters are said to no longer have any WINS requirements
- ▶ If you want to install WINS, then don't look in 2008's "Roles," as WINS is a "Feature"
- ▶ One big issue: IPv6 doesn't have a clue about WINS/NetBIOS and vice versa

4

4

The Browser, Though...

- ▶ Service is disabled by default in a workgroup system, even if it has shares
- ▶ Browser replacement: Network Discovery, off by default
- ▶ Driven by multicast messages, not broadcasts

5

5

Network Discovery Details

- ▶ Built along Universal PnP lines
- ▶ Advertisements/announcements go to multicast address 239.255.255.250 (which is, note, not a local-only address)
- ▶ Driven by Web Services Dynamic Discovery or WS-Discovery standard (different sources use different acronyms – WSSD or WSD)
- ▶ Uses UDP port 3702, TCP port 5357 (HTTP), TCP port 5358 (HTTPS)

6

6

Changes to DNS Internals

(well, really only one change)

7

DNS Server Changes

background zone loading

- ▶ Really only one: a serious performance improvement
- ▶ Problem: when a 2003 DNS server loads a large number of Active Directory-integrated zones upon boot, the DNS server may take (in some cases) an hour to be able to resolve names
- ▶ Meanwhile, AD is also loading, and needing queries resolved
- ▶ 2003 DNS cannot respond to any queries until all AD-I zones loaded
- ▶ Not a problem with primary/secondary zones

8

8

DNS Server Changes

pre-2008 process

- ▶ 2003 DNS does this in order:
 - ▶ Enumerate zones
 - ▶ Load root hints
 - ▶ Load zone files (*.dns text files in system32\dns)
 - ▶ Open RPC port for queries
 - ▶ Then load AD-integrated zones
- ▶ This is all pretty fast, but on a system with tons of DNS information in AD, it can mean that a DNS server can't respond to queries for some time, leading to the obvious troubles

9

9

DNS Server Changes

the fixes

- ▶ DNS is now multithreaded, so it needn't wait for that whole process to start responding to queries
- ▶ If DNS sees that it isn't yet able to answer queries on AD-I zones but queries are coming in, DNS just does an LDAP query to some other DC to resolve a DNS query
- ▶ Can't accept updates until all zones are loaded

10

10

Administering DNS in 2008

11

Installing DNS in 2008

- ▶ From the GUI: Server Manager, as a role
- ▶ From the CLI on a full server:
 - ▶ `servermanagercmd –install DNS`
- ▶ From the CLI on Server Core
 - ▶ `ocsetup DNS-Server-Core-Role`
 - ▶ Case matters for `ocsetup`!

12

12

DNS and Server Core

- ▶ Server Core requires CLI tools
- ▶ DNSCMD is now "in the box"
- ▶ Netsh lets you set preferred DNS servers:
- ▶ `netsh int ip set dns "local area connection" static 192.168.1.11`
- ▶ `netsh int ip add dns "local area connection" 192.168.1.12 index=2`
- ▶ Use all of "Local Area Connection" with netsh in 2008 due to IPv6 conflicts (or rename your NICs to something shorter... GP settings can do this)

13

13

DNS CLI Administration

examples of dnscmd in 2008 Server Core

- ▶ `dnscmd /zoneadd bigfirm.com /primary`
- ▶ Creates a zone named "bigfirm.com" on the local DNS server, stores it as a primary zone in a zone file named bigfirm.com.dns, and sets the zone to not allow dynamic updates
- ▶ `dnscmd /zonedel delete bigfirm.com /f`
- ▶ Deletes bigfirm.com, force delete
- ▶ `dnscmd /config bigfirm.com /allowupdate 1`
- ▶ Tells bigfirm.com to accept dynamic updates

14

14

DNS CLI Administration

examples of dnscmd in 2008 Server Core

- ▶ `dnscmd /enumzones`
- ▶ Displays all zones on this system
- ▶ `dnscmd /recordadd bigfirm.com S1 A 10.1.1.3`
- ▶ Adds the "A" record "S1 A 10.1.1.3" to the bigfirm.com zone
- ▶ `dnscmd /recorddelete bigfirm.com S1 A 10.1.1.3`
- ▶ Deletes the A record

15

15

DNS and AD Setup/Admin Changes

16

DNS and AD Setup

- ▶ As before,
 - ▶ AD requires a dynamic DNS infrastructure
 - ▶ You can avoid DDNS by collecting and copying the netlogon.dns files into a BIND-compatible zone file (my favorite form of e-masochism)
 - ▶ AD-integrated DNS works as before
 - ▶ You will still want a DNS reverse lookup zone to facilitate site-based group policy objects and to quell DDNS chatter on PTR records

17

17

DNS and AD Setup

- ▶ Changes:
 - ▶ You can make a Server Core system a DNS server (and a DC or RODC, for that matter)
 - ▶ DNSCMD is no longer an optional admin tool, it's in the box

18

18

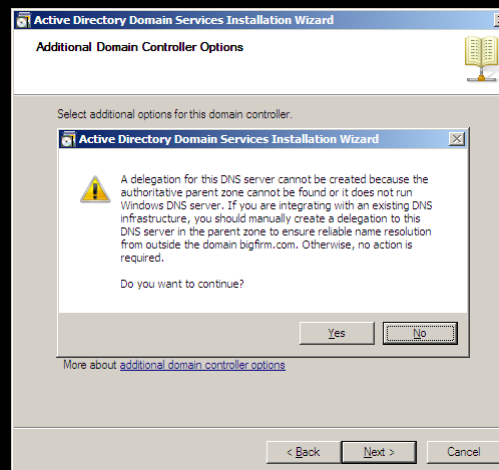
DNS and DCPROMO

- ▶ DCPROMO now talks a lot more about DNS
- ▶ It features two pages in its wizard that may be a bit confusing if not read right
- ▶ New definitions:
 - ▶ If you create an AD called "bigfirm.com," then "bigfirm.com" is called the "authoritative parent zone"
 - ▶ _msdcs.bigfirm.com is now called "the delegation"
 - ▶ Take a look:

19

19

DNS and 2008 DCPROMO



This error appears if you haven't created the zone and it wants to install DNS; does not in the other two options – means it can't find bigfirm.com

Note that all DCs are GCs by default, and now there's a check box to tell dcpromo to install DNS

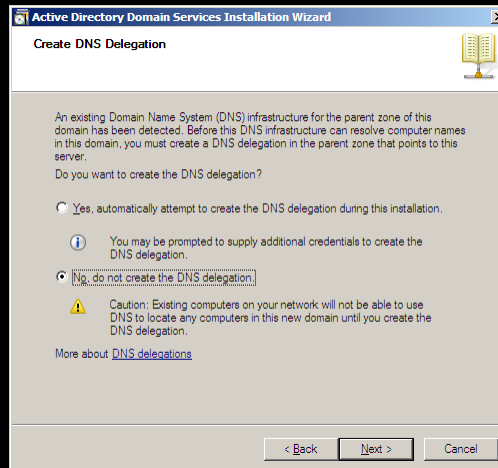
20

20

DNS and 2008 DCPROMO

"how should I create _msdcs?"

This *always* gets asked, even *if* you've already created the `_msdcs` zone



If you click "yes," you'll be asked to log in to authorize the DNS mods, and if you click "no..."

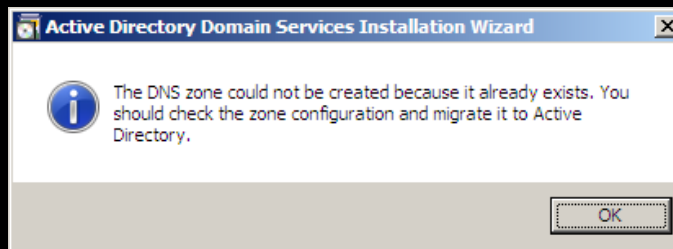
21

21

DNS and 2008 DCPROMO

problem: harder auto-reboot DCPROMO

- Once DCPROMO starts configuring AD, you'll get this (which stops everything):



Arggh. Of course it already exists, you ninny; that's why I clicked "no" in the "Create DNS Delegation" page. (It's about `_msdcs`.)

22

22

DNS and 2008 DCPROMO

avoiding pain

- ▶ You can avoid the pointless info box by either
 - ▶ Telling DCPROMO to set up AD-I zones
 - ▶ Adding `"/skipautoconfigdns"` to `dcpromo`
 - ▶ Adding `/unattend:filename` and an unattended DCPROMO install file
- ▶ And note a quirk in 2008's DNS server:
 - ▶ Set up a DNS server
 - ▶ Create a primary dynamic zone
 - ▶ Will not accept dynamic updates until you've stopped and started the DNS service

23

23

Read-Only DCs and DNS

- ▶ Think of RODCs as more vulnerable to compromise, and consider...
- ▶ In 2000/2003, any DC can (of course) modify an AD-integrated zone
- ▶ So in LH, RODCs cannot directly modify ADI zones by default -- they authenticate to an RWDC to "relay" the dynamic update
- ▶ They can, of course, host their own DDNS zones

24

24

What if You Don't Like That?

- ▶ Just go to the ADI zone object in question in AD
- ▶ Modify the zone's permissions to allow that particular DC to write to the zone
- ▶ Use ADSIEDIT and no, you can't see a permission like that in 2003
- ▶ Remember that a server's real name is the servername with a "\$" suffixed
- ▶ That lets an RODC directly update any given zone

25

25

DNS Client Changes

Finding DCs better

26

Using DNS to Re-Find DCs

- ▶ Old Problem: sometimes we're logged on by distant DCs due to network traffic in the A.M.
- ▶ Not a terrible thing, but it can slow things down and chew up bandwidth
- ▶ We've had answers like setprfdc (NT SP3) or netdom:
- ▶ `netdom reset mypc /domain:bigfirm.com`
- ▶ But it'd be nice to do this automatically

27

27

Review: How'd We Get Here?

- ▶ At startup, your PC grabs two lists of DCs:
 - ▶ just the local DCs
 - ▶ all DCs, no matter their location
- ▶ Ideally a local DC responds and logs your system on, but again due to congestion may not happen
- ▶ Here's the biggie: whichever "nearest responding DC" you find, that's the one that's cached and will therefore be the first place you look for re-logons

28

28

How 2008/Vista Rediscover

- ▶ You can make the cache "evaporate" after a given time
- ▶ Works for Vista and 2008 – no such client control on XP, 2003
- ▶ In Group Policies: Computer Configuration\Administrative templates\System\Netlogon\DC Locator DNS Records\Force Rediscovery Interval (in seconds)
- ▶ Registry:
HKLM\Software\Policies\Microsoft\Netlogon\Parameters!ForceRediscoveryInterval

29

29

Smarter DC Discovery Part 2

- ▶ Remember how we find DCs -- first local DCs, then all DCs (global list)
- ▶ Vista and 2008 systems can behave differently:
 - ▶ First get the local list
 - ▶ If no DCs responded, then ask for the next nearest site
 - ▶ Get the list of DCs there
 - ▶ If none respond, get global list and query those DCs

30

30

Making it Work

- ▶ Actual query goes to inter-site topology generator
- ▶ This behavior doesn't by default
- ▶ Enable with Registry change
- ▶ HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\
 - ▶ REG_DWORD TryNextClosestSite
 - ▶ 0 = don't use next site 1 = do use next site

31

31

Name Resolution in IPv6

just a few words for a big topic

Name Resolution in IPv6

to start off...

- ▶ No NetBIOS support at all
- ▶ IPv6 doesn't use or understand WINS
- ▶ And for local name resolution...

33

IPv6 Name Resolution

local name resolution

- ▶ Name resolution on a link happens through multicasts "link local multicast name resolution" (LLMNR)
- ▶ Documented in RFC 4795
- ▶ Requester multicasts to address FF02::1:3 on UDP port 5335
- ▶ Answerer unicasts to requester on UDP 5335
- ▶ Can query for any DNS record type
- ▶ Does not need any DNS servers, however

34

IPv6 and AAAA

- ▶ We all know A ("host") records, which map host names to IPv4 addresses
- ▶ IPv6 brings AAAA ("quad-A") records, which map host names to IPv6 addresses
- ▶ Vista and 2008's DNS clients automatically register AAAAs
- ▶ However, note that the link-local addresses that start with "FE80" do not register themselves in DNS
- ▶ DNS Server in 2003 handles AAAAs just fine

35

35

Meet the New Record Types

AAAA (okay, you've already met that one), DNAME, and GlobalNames

36

DNAME: Simplifying Migration

- ▶ So let's suppose you're going to rename your enterprise from "minasi.com" to "bigfirm.com"
- ▶ You've got to find every single "minasi.com" reference in the Registry and other configuration places and change them to "bigfirm.com"
- ▶ Ugh.
- ▶ How to make this happen more quickly?

37

37

The Answer: minasi->bigfirm

- ▶ So imagine you could say to your DNS server, "whenever anyone asks for something.minasi.com, just look up something.bigfirm.com and return that answer"
- ▶ In some senses it's kind of like what a familiar CNAME ("alias") does in DNS currently: "when someone asks for www.minasi.com, give 'em s2.dom.com"

38

38

It's Even Standards-Based

- ▶ DNS techies will know that the record type for host aliases is called, again, a CNAME record
- ▶ RFC 2672 defined a "domain alias" record, a "DNAME" record
- ▶ RFC says, "no descendant nodes in the old domain" (that is, remove everything but the NS, SOA and similar – no As, AAAAs, CNAMEs etc)
- ▶ Then place the DNAME record in the minasi.com zone
- ▶ Clearly this will help with domain renames

39

39

Details

- ▶ Put the DNAME record in the old domain
- ▶ It should point to the new domain
- ▶ For example: to go minasi.com->bigfirm.com
 - ▶ Edit the minasi.com zone
 - ▶ Add a record "minasi.com. DNAME bigfirm.com."
 - ▶ Effect: looking up www.minasi.com on the DNS server will return the A record of www.bigfirm.com

40

40

Doing It

- ▶ No GUI!
- ▶ `dnscmd /recordadd minasi.com @ DNAME bigfirm.com.`
- ▶ Or hack the zone file directly:
- ▶ `@ DNAME bigfirm.com.`
- ▶ Be very careful which domains you do it for, though!

41

41

Trying it out

- ▶ This works:
- ▶ `dnscmd /zoneadd minasi.com /primary`
- ▶ `dnscmd /zoneadd bigfirm.com /primary`
- ▶ `dnscmd /recordadd bigfirm.com Sys1 A 10.10.10.3`
- ▶ `dnscmd /recordadd minasi.com @ dname bigfirm.com`
- ▶ `nslookup sys1.minasi.com`

42

42

Gotcha...

- ▶ This doesn't work:
- ▶ `dnscmd /zoneadd minasi.com /primary`
- ▶ `dnscmd /zoneadd bigfirm.com /primary`
- ▶ `dnscmd /recordadd minasi.com C1 A 10.10.10.1`
- ▶ `dnscmd /recordadd minasi.com @ dname bigfirm.com <--- FAILS`
- ▶ Why? Can't have records in the now-vacated minasi.com zone except the dname

43

43

So how does it work?

- ▶ A DNS client makes a request to the DNAME-aware server
- ▶ DNAME-aware server reformulates the request for the "A" record for server3.minasi.com to a response that "server3.minasi.com" is just a CNAME for "server3"
- ▶ From there, it's pretty much business as usual

44

Post-WINS Single Label Names

- ▶ Or, in English...
- ▶ The one really great thing about WINS was that we could refer to a server by a name like server44 rather than server44.eastcoast.sales.bigfirm.com
- ▶ In a single domain AD world, we still have that feature
- ▶ But what about other environments?

45

45

Doing Single-Label (In 2003)

- ▶ You can deploy a DNS suffix search list via GPOs (Computer Config / Admin Templates / Network / DNS Client)
- ▶ But...
 - ▶ What if there are multiple server44s?
 - ▶ No matter how many DNS suffixes your client has, it stops trying DNS resolutions after 12 seconds and then goes to WINS
 - ▶ You might not have control over this GPO setting

46

46

Doing Single-Label in 2008 create GlobalNames

- ▶ Create a zone named "GlobalNames"
- ▶ All DNS servers authoritative for it must be Server 2008 <-- big "if!"
- ▶ On each DNS server holding the zone, enable global name resolution:
`dnscmd /config /enableglobalnamesupport 1`

47

47

Doing Single-Label in 2008 add entries

- ▶ Now add CNAMEs
- ▶ For example, to ensure that "server44" always returns the address server44.sales.bigfirm.com, create this in GlobalNames:
- ▶ `server44 CNAME server44.sales.bigfirm.com`

48

48

Requirements

- ▶ Again, all authoritative servers must be 2008
- ▶ Possible to use a primary zone file, but AD-I is better
- ▶ Placing it in ForestDNSZones also makes the most sense in most cases
- ▶ Well worth looking into!

49

49

Thanks For Joining Me!

- ▶ I'm at help@minasi.com
- ▶ My Web site is www.minasi.com
 - ▶ free technical newsletter there
 - ▶ online forum there as well
 - ▶ Info on my two-day Vista and 2008 support seminars as well
- ▶ Please fill out an evaluation!

50

50