## CONFIGURE DNS SERVER PROPERTIES2

DNS is fairly simple and straightforward. As long as you follow the basic rules of configuration, DNS will give you few problems. However, there are certain complex configurations that are important to know about and remember. This article exposes the details of DNS server properties, which will allow administrators to get a better handle on options that can make a difference in DNS operation, logging and troubleshooting.

One of the first things I had to figure out when I learned DNS in Active Directory was how to remember if a property was that of the DNS server or a zone. Both are exposed in the DNS Management snap-in tool.

DNS server properties are exposed by right-clicking on the DNS server icon as shown in Figure 1. Zone properties, on the other hand, are found if you right-click on a particular zone name under Forward or Reverse Lookup Zones.

Here are a couple of ways to keep them straight:

• Server properties are general properties that apply to the whole DNS environment, such as Forwarding, Name Servers, root hints and logging.

• Zone properties are specific properties that vary with the zone, such as dynamic updates, zone type (AD, Standard Primary or Secondary) and replication type.

Figure 1: DNS server properties and the DNS server icon



#### The DNS Server Properties page

Let's take a closer look at the server properties. Figure 2 shows the DNS Server Properties page, with eight tabs, followed by a description of features included for each of those eight areas.

disengent - [DNS\WTEC-DCT\Forward Looku	p Zunes]
🕺 File Action View Window Help	
◆ → 🗈 🗷 🗗 🕄 🖉 🗐 🖓	WTEC-DC1 Properties ? X
DNS     WTEC-DC1     Forward Lookup Zones     G_medes.Wtec.adapps.hp.com     G_Wtec.adapps.hp.com     G_Wtec.adapps.	Debug Logging     Event Logging     Monitoring     Security       Interfaces     Forwarders     Advanced     Root Hints       Select the IP addresses that will serve DNS requests. The server can listen for DNS gueses on all P addresses.     E Dree       Listen or: <ul> <li>Add</li> <li>Diff addresses</li> <li>Brenowy</li> <li>Brenowy</li> <li>Diff Tablesses</li> <li>Diff Cancel</li> <li>Drev</li> <li>Dreve</li> <li>Dreve</li> <li>Drev</li> <li>Dreve</li> <l< td=""></l<></ul>

# Figure 7. DNS Somer Properties nage

#### *Interfaces*

There are several reasons to configure multiple interfaces for DNS. If you have a multi-homed DNS server and want to configure DNS to use only one of the NICs, then configure it here in the "Listen on" section by selecting the "only the following IP addresses" option, then listing the address(es). This could be an issue for two reasons: One, you add a new NIC and intend to keep both NICs, but you only want the new one to be used for DNS traffic or, two, if the old NIC was mistakenly left in.

Another use for this configuration is for preventing hosts outside the subnet or routed subnets from accessing the DNS server.

#### *Forwarders*

For most administrators, this tab should be the most familiar. Forwarders are required to forward DNS referrals to resolve names for which the current DNS server knows nothing about. If a client in the corp.net zone needs to resolve a name in the emea.corp.net zone, the DNS server in corp.net must forward to another DNS server that can ultimately resolve the name. Failure to find such a DNS server will result in failure of the query for the client.

In Windows Server 2003, Microsoft added a new feature called Conditional Forwarding. This title does not appear in any of the property tabs, but it is configured on the Forwarding tab. Figure 3 shows the Conditional Forwarding configuration fields circled in red. Again, it doesn't say Conditional Forwarding, it simply says "DNS Domain." This feature allows you to specify a DNS server that can handle a domain. For instance, in Figure 3, the DNS server is in the WTEC.Adapps.hp.com domain. We have specified the domain HPQBOX.adapps.HP.Com (another forest) and entered IP addresses of two DNS servers that are authoritative for the HPQBOX domain. Thus, instead of following normal forwarding (going up and down the DNS tree), this configuration takes a shortcut right to the HPQBOX domain's DNS servers. You can enter multiple domains and multiple DNS servers per domain.

Debug Logging Interfaces	Event Logging Forwarders	Monitoring Advanced	Root Hints
orwarders are serve erver. Forward quer	rs that can resolve DN ies for names in the fo	IS queries not ar lowing DNS dom	nswered by this nains.
DNS domain:			
All other DNS doma	ins		<u>N</u> ew
nr goox.adapps.hp	com		D
			and the second se
o add a forwarder,	select a DNS domain,	type the forward	er's IP address
o add a forwarder, s below, and then click	select a DNS domain, < Add. rwarder IP address list	type the forward	er's IP address
o add a forwarder, below, and then click belected domain's fo	select a DNS domain, < Add. rwarder I <u>P</u> address list Add	type the forward	er's IP address
o add a forwarder, below, and then click belected domain's fo	select a DNS domain,	type the forward	er's IP address
o add a forwarder, below, and then click selected domain's fo 10.12.7.122 10.12.8.125	select a DNS domain, k Add. inwarder IP address list Add Bernove Up	type the forward	er's IP address
To add a forwarder, s below, and then click Selected domain's fo 10.12.7.122 10.12.8.125	select a DNS domain, k Add. inwarder IP address list Add Bernove Up Dgwn	type the forward	er's IP address
To add a forwarder, selow, and then click Selected domain's fo 10.12.7.122 10.12.8.125	select a DNS domain, Add. Inwarder IP address list Add Elemove Up Down before forward queries	type the forward	er's IP address

Figure 3: Conditional Forwarding feature in action

At the bottom of the Forwarders page there is a check box: Do Not Use Recursion for this Domain. In Windows 2000, it simply read "Do Not Use Recursion."

## Advanced

The Advanced tab, shown in Figure 4, contains settings that, in reality, you will probably never use. The help file found in the DNS Management snap-in has a detailed description of these options under the heading "Tuning Advanced Server Parameters." Some of these options are described below.

# Figure 4: Advanced tab settings

Debug Logging	Event Logg	ing   1	Monitoring	Security
Interfaces	Forwarders	Adva	nced	Root Hints
Server version num	iber:			
5.2 3790 (0xece)				
Server options:				
Disable recursio	n (also disables fo	rwarders)		
BIND secondari	ies			
🗌 Fail on load if ba	ad zone data			
Enable round to	hin			
Chaple round to	Diri			
Enable netmask	ordering			
<ul> <li>Enable netmask</li> <li>Secure cache a</li> </ul>	ordering against pollution			
<ul> <li>Enable notmask</li> <li>Secure cache a</li> </ul>	ordering against pollution			
v Enable noting to v Enable notings v Secure cache a Name checking:	s ordering against pollution	ultibyte (UT	F8)	-
♥ Enable noting to ♥ Enable netmask ♥ Secure cache a Name checking _oad zone data on	sordering against pollution M startup: Fr	ultibyte (UT om Active [	F8) Directory and	∎ d registry
✓ Enable notation ✓ Enable netmask ✓ Secure cache a Name checking Load zone data on ✓ Enable automa	sordering against pollution startup: Fr tic scavenging of	ultibyte (UT om Active [ stale record	F8) Directory and	∎ d registry
Enable notation     Enable notation     Enable netmask     Secure cache a     Mame checking:     Load zone data on     Enable automa     Sgavenging pe	sordering against pollution startup: Fr tic scavenging of riod: 1	ultibyte (UT om Active [ stale record	F8) Directory and	d registry
<ul> <li>Enable notation</li> <li>Enable netmask</li> <li>Secure cache a</li> <li>Mame checking</li> <li>Load zone data on</li> <li>Enable automa</li> <li>Scavenging pe</li> </ul>	sordering against pollution startup: Fr tic scavenging of riod: 1	ultibyte (UT om Active [ stale record	F8) Directory and Is days	d registry
<ul> <li>Enable notation</li> <li>Enable netmask</li> <li>Secure cache a</li> <li>Name checking:</li> <li>Load zone data on</li> <li>Enable automa</li> <li>Scavenging pe</li> </ul>	sordering against pollution startup: Fr tic scavenging of riod: 1	ultibyte (UT om Active [ stale record	F8) Directory and Is days Rese	d registry

• *Disable Recursion* -- Recursion occurs when a DNS server cannot resolve a DNS query by a client and uses other DNS servers to help resolve it. This can involve the root servers at the root of the Internet naming tree, thus giving each DNS server the ability to find any name on the Internet. Recursion is when a DNS server resolves a name on behalf of a client, then returns the result to the client. Iteration is when the client does all the work itself.

This option is not checked (thus enabling recursion) by default. If you check this option, it will disable forwarders, so be careful. While this would seem to be a bad idea normally, you might want to disable recursion if you want to restrict clients to resolving names on a particular DNS server, or where you want to restrict access to the Internet for security reasons. Note: This operation can be accomplished by checking the "Do not use Recursion for this domain" checkbox on the Forwarders tab.

• *Fail on load if bad zone data* -- This really only applies to a "standard" type zone (not AD integrated). I've used it a couple of times when a DNS zone appeared to be corrupt. It will prevent loading of the zone and log errors.

• *Secure cache against pollution* -- Windows 2000 had a number of cache issues. This option allowed us to prevent possible inaccurate entries such as getting a referral from a server outside of the domain we queried. If it was allowed to cache, then it could cause name resolution problems. To be honest, I've only seen a handful of DNS cache problems and I haven't used this option to correct them. Instead, I cleared the server cache until I resolved the real DNS problem.

The Server Cache clearing option is exposed by right clicking on the DNS server icon in the DNS Management snap-in and selecting Clear Cache.

• *Reset to Default* -- Selecting this button clears all the bad decisions you made in this tab and restores the default settings.

• *Enable Automatic Scavenging of Stale Records* -- With this setting, you can define scavenging parameters. It deletes DNS records that have not been updated in a defined period of time. Be careful with this one. While it is a good thing to scavenge stale records, if you are using third-party DNS tools that don't properly update your Windows DNS servers, you could scavenge valid, active records.

#### **Root Hints**

Root Hints is a list of all DNS servers at the root of the Internet and is used in recursive name resolution. On this tab, there is an ADD button that allows you to build custom root hints. The only experience I've had with custom root hints has been bad. Folks will configure a particular DNS server to serve as a root hint, but then it gets misconfigured or the IP address changes, and you forget that it's there, which can cause troubleshooting problems and DNS errors. My recommendation: Do not build custom root hints.

#### Debug Logging

Figure 5 shows all the options on this tab if you check the "log packets for debugging" option. It is a decent option to use if you don't want the hassle of setting up a network trace and are limited to DNS packets. Note: At the bottom of this page, you can configure the size and location of the DNS log. If this size is exceeded, it will overwrite itself. The log is located at %windir%\system32\dns\dns.log.

# Figure 5: Debug Logging options

Interfaces	Forwarders	Advanced	Root Hints
Debug Logging	Event Loggin	g Monitori	ng Security
To assist with debu the DNS server to a ✓ Log packets for	gging, you can reco log file. Debug log debugging	ord the packets si ging is disabled b	ent and received by y default.
Packet direction: Cutgoing Lincoming	} select at least one	Transport proto	icol:   select at   least one
Packet contents: ▼ <u>Q</u> ueries/Transfe ▼ Update <u>s</u> ■ <u>N</u> otifications	ers } select at least one	Packet type: I▼ Requ <u>e</u> st I▼ <u>R</u> esponse /	select at least one
Other options: Details Filter pa <u>c</u> kets by Log file	v IP address	<u>Fi</u> lter	
File pat <u>h</u> and nam <u>M</u> aximum size (by	ne: 500000000		
	OK	Com	

## >Event Logging

This one is pretty simple. The default is to log all events, but it can be restricted to No Events, Errors Only or Errors and Warnings. I've never set this at anything other than the default because there are typically very few DNS events in the DNS event log. Name resolution (DNS Lookup) failures are usually reported as part of other events, such as the Event 1311 recorded in the directory services log for replication failure.

#### Monitoring

This is quite a handy tool when you are troubleshooting DNS problems. Figure 6 shows an example.

# Figure 6: Monitoring

Interfaces	Forwarders	Adv	anced	Root Hints
Debug Logging	Event Lo	ogging	Monitoring	Securi
To verify the con automatic testing Select a test type	figuration of the : ::	server, you ca	n perform m	anual or
✓ A simple que	ry against this DN	IS server		
A recursive q	uery to other DN	S servers		
	an actuar			-
a manharma black bar	al management of the last of	Kell, Teach Marry	- C C C	I net blow
I o perform the te	est immediately, c	lick Test Now	67 C	Lest Now
Perform autor	est immediately, c	lick Test Now	l. Herval-	Lest Now
Dependence of the term of term	matic testing at th	lick Test Now ne following in	terval:	Lest Now
To perform the te Perform auto T <u>e</u> st interval:	matic testing at the string of the string at the string of	lick Test Now ne following in nutes	terval:	Lest Now
To perform the te Perform autor Test interval: Test results:	est immediately, c matic testing at th 1 mi	lick Test Now ne following in nutes	terval:	est Now
Toperform the te <u>P</u> erform autor T <u>e</u> st interval: <u>Fest results:</u> Date	est immediately, c matic testing at th 1 mi Time	lick Test Now ne following in nutes	tervat V	Lest Now
Toperform the te ☐ Perform autor Test interval: Test results: Date 12/29/2006	est immediately, c matic testing at th 1 mi 7 mi 2:16:19 PM	lick Test Now ne following in nutes Simple Que Pass	terval:	est Now
To perform the te Perform autor Test interval: Test results: Date 12/29/2006	est immediately, c matic testing at th 1 mi <u>1 mine</u> 2:16:19 PM	lick Test Now ne following in nutes Simple Que Pass	terval:	rsive Q
To perform the te Perform autor Test interval: Test results: Date 12/29/2006	est immediately, c matic testing at th 1 mi 1 mi 2:16:19 PM	lick Test Now ne following in nutes Simple Que Pass	terval:	rsive Q
To perform the te Perform autor Test interval: Test results: Date 12/29/2006	est immediately, c matic testing at th 1 mi <u>1 mi</u> 2:16:19 PM	lick Test Now ne following in nutes Simple Que Pass	terval ery Recu Pass	rsive Q
Test interval: Test interval: Test 22006	est immediately, c matic testing at th 1 mi <u>Time</u> 2:16:19 PM	lick Test Now ne following in nutes Simple Que Pass	terval ry Recu Pass	rsive Q
To perform the te Perform autor Test interval: Test results: Date 12/29/2006	est immediately, c matic testing at th 1 mi <u>Time</u> 2:16:19 PM	lick Test Now ne following in nutes Simple Que Pass	terval:	rsive Q

Under "Select a test type" there are two check boxes: one for testing a simple query and one for testing a recursive query. Check one or both boxes, then select the Test Now button. If the test is successful, you will see "PASS" in the appropriate column under test results. Note: If the test is going to pass, it will return the results within a second or two. If you have to wait for it, it's probably going to fail.

The Simple Query tests name resolution for the zone loaded on this DNS server. The Recursive Query tests forwarding. Thus, if the simple query passes and the recursive query fails, then the problem is with forwarding.

If you get a failure, a yellow flag will appear on the server icon in the left-hand pane of the DNS management snap-in until you run a successful test. Just be aware that the monitor test produces that flag.

Yes, DNS is simple, but there are a number of options you can use, especially to aid in troubleshooting and taking forwarding shortcuts like conditional forwarding. Coming up, I will discuss zone properties, which are more likely to be changed.

Gary Olsen is a systems software engineer for Hewlett-Packard in Global Solutions Engineering. He authored <u>Windows 2000: Active Directory Design and Deployment</u> and coauthored <u>Windows Server 2003 on HP ProLiant Servers</u>.