

# Re: Forward Lookup Zone missing when new tree added to forest

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.dns/2006-11/msg00345.html>

---

- *From:* Shawn Conaway <[ShawnConaway@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:ShawnConaway@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 20 Nov 2006 13:44:01 -0800
- 

Hi,

Upon further review, DNS looks somewhat normal. There are lots of InProgress entries, but those were all made a year ago when AD was created. I don't show any weird entries from when I created the new domain last week.

"Shawn Conaway" wrote:

Is this what you meant by a bunch of numbers and letters in front of the zone? I have an abundance of "DC=..InProgress" entries. It looks like replication is wacked out by looking at all the InProgress entries. There are 11 of these entries, which is the same number as the domain controllers in the forest.

-----  
Name Class Distinguished Name

DC=..InProgress-42D512D5483B142F-fiserv.biz dnsZone

DC=..InProgress-42D512D5483B142F-fiserv.biz,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,DC=

DC=..InProgress-42D51481000815C3-Fiserv.Biz dnsZone

DC=..InProgress-42D51481000815C3-Fiserv.Biz,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,DC=

DC=..InProgress-42D5148600082A26-Fiserv.Biz dnsZone

DC=..InProgress-42D5148600082A26-Fiserv.Biz,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,DC=

DC=..InProgress-42D514E4001D4EAF-fiserv.biz dnsZone

DC=..InProgress-42D514E4001D4EAF-fiserv.biz,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,DC=

DC=..InProgress-42D65EAC0511CFDE-vision.fiserv dnsZone

DC=..InProgress-42D65EAC0511CFDE-vision.fiserv,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,DC=

DC=..InProgress-42D65F0505132ADA-vision.fiserv dnsZone

DC=..InProgress-42D65F0505132ADA-vision.fiserv,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,DC=

DC=..InProgress-42D662CD0002DC2D-fiserv.biz dnsZone

Re: Forward Lookup Zone missing when new tree added to forest

DC=..InProgress-42D662CD0002DC2D-fiserv.biz,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,DC=

DC=..InProgress-42D7D4E804590EA0-Fiserv.Biz dnsZone

DC=..InProgress-42D7D4E804590EA0-Fiserv.Biz,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,DC=

DC=..InProgress-42D7D5110459AE8A-vision.fiserv dnsZone

DC=..InProgress-42D7D5110459AE8A-vision.fiserv,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,D

DC=..InProgress-42DC129C163880D6-fiserv.biz dnsZone

DC=..InProgress-42DC129C163880D6-fiserv.biz,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,DC=

DC=..InProgress-42DC13790031F435-0.46.10.in-addr.arpa dnsZone

DC=..InProgress-42DC13790031F435-0.46.10.in-addr.arpa,CN=MicrosoftDNS,DC=ForestDnsZones,DC=F

DC=0.46.10.in-addr.arpa dnsZone

DC=0.46.10.in-addr.arpa,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,DC=biz

DC=1.46.10.in-addr.arpa dnsZone

DC=1.46.10.in-addr.arpa,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,DC=biz

DC=2.46.10.in-addr.arpa dnsZone

DC=2.46.10.in-addr.arpa,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,DC=biz

DC=fiserv.biz dnsZone

DC=fiserv.biz,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,DC=biz

DC=vision.fiserv dnsZone

DC=vision.fiserv,CN=MicrosoftDNS,DC=ForestDnsZones,DC=Fiserv,DC=biz

"Ace Fekay [MVP]" wrote:

In [news:6F57D33B-F357-4614-9175-59AC38A20C63@xxxxxxxxxxxxxxxxx](mailto:news:6F57D33B-F357-4614-9175-59AC38A20C63@xxxxxxxxxxxxxxxxx),  
Shawn Conaway <ShawnConaway@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> stated,  
which I  
commented on below:

Thanks Ace.

My replication looks like it is working fine. I added DNS to  
the  
second domain controller in my tree (10.3.1.104) and my  
DNS log is  
not showing errors any more. I am able to resolve names.

The real concern I have is that there is no forward lookup  
zone for  
shell.company listed in DNS on the forest root server or in

Re: Forward Lookup Zone missing when new tree added to forest

DNS for  
the domain controller in the sight.company domain.  
However, DNS on  
the shell.company domain controller shows both the  
sight.company and  
company.biz zones.

I expected AD-integrated DNS to replicate on its own  
without adding  
any forward lookup zones. However, the other two trees are  
AD-integrated as well and they do have forward lookup  
zones. There  
seems to be a mismatch there. I'd expect all forward lookup  
zones or  
none at all since it is all AD-integrated.

Although everthing appears OK, I'm going to run diagnostics  
to verify  
that DNS and AD replication are actually working so that the  
whole  
deal doesn't come to a screeching halt in 30 days. The lack of  
a  
forward lookup zone does have me worried.

Below is the ipconfig for the three servers:

\*\*\* Forest Root server \*\*\*

Host Name . . . . . : DC1  
Primary Dns Suffix . . . . . : company.Biz  
Node Type . . . . . : Hybrid  
IP Routing Enabled. . . . . : No  
WINS Proxy Enabled. . . . . : No  
DNS Suffix Search List. . . . . : company.biz  
sight.company  
mke.company.net  
companysolutions.com

Ethernet adapter 10.3.1.244:

Connection-specific DNS Suffix . : company.Biz  
Description . . . . . : AMD PCNET Family PCI  
Ethernet  
Adapter Physical Address. . . . . :  
00-0C-29-D2-64-C8  
DHCP Enabled. . . . . : No  
IP Address. . . . . : 10.3.1.244  
Subnet Mask . . . . . : 255.255.252.0  
Default Gateway . . . . . : 10.3.0.1  
DNS Servers . . . . . : 10.3.1.244

Re: Forward Lookup Zone missing when new tree added to forest

10.3.1.239  
10.3.1.103  
Primary WINS Server . . . . . : 10.3.1.239

---

\*\*\* Second tree in domain \*\*\*

Host Name . . . . . : DC3  
Primary Dns Suffix . . . . . : sight.company  
Node Type . . . . . : Hybrid  
IP Routing Enabled. . . . . : No  
WINS Proxy Enabled. . . . . : No  
DNS Suffix Search List. . . . . : sight.company  
company.biz  
mke.company.net  
shell.company

Ethernet adapter 10.3.1.239:

Connection-specific DNS Suffix . : sight.company  
Description . . . . . : AMD PCNET Family PCI  
Ethernet  
Adapter Physical Address. . . . . :  
00-0C-29-AB-15-F8  
DHCP Enabled. . . . . : No  
IP Address. . . . . : 10.3.1.239  
Subnet Mask . . . . . : 255.255.252.0  
Default Gateway . . . . . : 10.3.0.1  
DNS Servers . . . . . : 10.3.1.239  
10.3.1.244  
10.3.1.103  
Primary WINS Server . . . . . : 10.3.1.239  
Secondary WINS Server . . . . . : 10.3.0.15

---

\*\*\* New tree in domain \*\*\*

Host Name . . . . . : DC8  
Primary Dns Suffix . . . . . : shell.company  
Node Type . . . . . : Hybrid  
IP Routing Enabled. . . . . : No  
WINS Proxy Enabled. . . . . : No  
DNS Suffix Search List. . . . . : company.biz  
sight.company  
mke.company.net  
companysolutions.com  
shell.company

Re: Forward Lookup Zone missing when new tree added to forest

Re: Forward Lookup Zone missing when new tree added to forest

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : shell.company  
Description . . . . . : VMware Accelerated AMD  
PCNet  
Adapter Physical Address. . . . . : 00-50-56-B0-30-A2  
DHCP Enabled. . . . . : No  
IP Address. . . . . : 10.3.1.103  
Subnet Mask . . . . . : 255.255.252.0  
Default Gateway . . . . . : 10.3.0.1  
DNS Servers . . . . . : 10.3.1.103 (self)  
10.3.1.104 (DC2 --> second DC in  
shell.company)  
10.3.1.244 (forest root)  
10.3.1.239 (DC for second tree  
in forest)  
Primary WINS Server . . . . . : 10.3.1.239

Thanks for posting the additional information.

It appears ok, but what worries me is the shell.company zone is not appearing as you stated. If the replication scope is set to forest wide, then all DC/DNS servers will have a copy.

Check using ADSI Edit to confirm that the zone actually exists in the ForestDnsZones partition. If you see a zone name with a bunch of numbers/letters in front of it, then it means there's a dupe, which will cause problems.

Here is some additional info on how to do that and what can happen if there is any problems. This is from my own private blogs which I have not yet published. Some of it may apply and relate, other parts may not. I hope it helps.

=====  
=====

Conflicting AD Integrated zones if they exist in both the Domain NC and one of the Application Partitions or if you get a weird error message stating:  
"The name limit for the local computer network adapter card was exceeded."

Under Windows 2000, the physical AD database is broken up into 3 logical partitions, the DomainNC (Domain Name Context, or some call the Domain Name Container), the Configuration Partition, and the Schema Partition. The Schema and Config partitions replicate to all DCs in a forest. However, the DomainNC is specific only to the domain the DC belongs to. That's where a

Re: Forward Lookup Zone missing when new tree added to forest user, domain local or global group is stored. The DomainNC only replicates to

the DCs of that specific domain. When you create an AD INtegrated zone in Win 2000, it gets stored in the DomainNC. This causes a limitation if you want

this zone to be available on a DC/DNS server that belongs to a different domain. The only way to get around that is for a little creative designing using

either delegation, or secondary zones. This was a challenge for the \_msdcs zone, which must be available forest wide to resolve the forest root domain,

which contains the Schema and Domain Name Masters FSMO roles.

In Windows 2003, there were two additional partitions added, they are called the DomainDnsZones and ForestDnsZones Application Partitions, specifically

to store DNS data. They were conceived to overcome the limitation of Windows 2000's AD Integrated zones. Now you can store an AD Integrated zone in

either of these new partitions instead of the DomainNC. If stored in the DomainDnsZones app partition, it is available only in that domain's

DomainDnsZones partition. If you store it in the ForestDnsZones app partition, it will be available to any DC/DNS server in the whole forest. This opens

many more design options. It also ensures the availability of the \_msdcs zone to all DCs in the forest. By default in Win 2003, the \_msdcs zone is stored in

the ForestDnsZones application partition.

When selecting a zone replication scope in Win2003, in the zone's properties, click on the "Change" button. Under that you will see 3 options:

To choose the ForestDnsZones:

"To all DNS serer in the AD forest example.com"

To choose DomainDnsZones:

"To all DNS serer in the AD domain example.com"

To choose the DomainNC (only for compatibility with Win2000):

"To all domain controllers in the AD domain example.com"

If you have a duplicate, that's telling me that there is a zone that exists in the DomainNC and in the DomainDnsZones Application partition. This

Re: Forward Lookup Zone missing when new tree added to forest

means  
at

one time, or currently, you have a mixed Win2000/2003 environment and you have DNS installed on both operating systems. On Win2000, if the zone is

AD Integrated, it is in the DomainNC, and should be set the same in Win2003's DC/DNS server to keep compatible. Someone must have attempted to

change it in Win2003 DNS to put it in the DomainDnsZones partition realizing the implications, hence the duplicate. In a scenario such as this where

you want to use the Win2003 app partitions, you then must insure the zone on the Win2003 is set to the DomainNC, then uninstall DNS off the Win2000

machine, then once that's done, you can then go to the Win2003 DNS and change the partition's replication scope to one of the app partitions.

In ADSI Edit, you can view all five partitions. You were viewing the app partitions, but not the main partitions. You need to add the DomainNC partition in

order to delete that zone. But you must uninstall DNS off the Win2000 server first, unless you want to keep the zone in the DomainNC. But that wouldn't

make much sense if you want to take advantage of the \_msdcs zone being available forest wide in the ForestDnsZones partition, which you should

absolutley NOT delete. I would just use the Win2003 DNS servers only.

In ADSI Edit, rt-click ADSI Edit, connect to, in the Connection Point click on "Well known Naming Context", then in the drop-down box, select "Domain".

Drill down to CN=System. Under that you will see CN=MicrosoftDNS. You will see the zone in there.

But make sure to decide FIRST which way to go before you delete anything.

Some reading for you...

Directory Partitions:

[http://www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/distrib/dsbg\\_c](http://www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/distrib/dsbg_c)

kbAlertz- (867464) - Explains how to use ADSI Edit to resolve app partitions issues:

Re: Forward Lookup Zone missing when new tree added to forest

[http://www.kbalertz.com/kb\\_867464.aspx](http://www.kbalertz.com/kb_867464.aspx)

How to fix it?

-----

What I've done in a few cases with my clients that have issues with 'duplicate' zone entries in AD (because the zone name was in the Domain NC (Name Container) Partition, and also in the DomainDnsZones App partition), was first to change the zone on one of the DCs to a Primary zone, and allowed zone transfers. Then I went to the other DCs and changed the zone to a Secondary, and using the first DC as the Master. Then I went into ADSI Edit, (from memory) under the Domain NC, Services, DNS, and deleted any reference to the domain name. Then I added the DomainDnsZones partition to the ADSI Edit console, and deleted any reference to the zone name in there as well. If you see anything saying something to the extent of "In Progress..." with a long GUID number after it, delete them too. Everytime you may have tried to change the replication scope, it creates one of them. Delete them all.

Then I forced replication. If there were Sites configured, I juggled around the servers and subnet objects so all of the servers are now in one site, then I forced replication (so I didn't have to wait for the next site replication schedule). Once I've confirmed that replication occurred, and the zones no longer existed in either the Domain NC or DomainDnsZones, then I changed the zone on the first server back to AD Integrated, choosing the middle button for it's replication scope (which puts it in the DomainDnsZones app partition). Then I went to the other servers and changed